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

© Користін О.Є., ДНДІ, ОДУВС 2024

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

FOREWORD



Ukraine's Law Enforcement Agencies (LEA) are facing uniq-ue challenges – contributing to the defence of the country against the Russian war of aggression while ensuring the functioning, and reform, of the civilian security sector. The LEA have shown remarkable resilience and commitment to function and improve despite these enormous trials.

The Overarching Strategic Plan for Reforming Law Enforcement Agencies in Ukraine (OAS), approved by President Zelenskyy in May 2023, includes priorities such as the extension of interagency cooperation as well as increasing efficiency of LEA in the performance of their functions and improving inter-agency cooperation. The strategic plan also foresees ensuring further development of the system of LEA based on the use of risk-oriented approaches, a focus on information and analytical activity, strategic management, and forecasting. The importance of identifying annual priority areas for combatting crime based on crime rates, structure, dynamics and trends is also highlighted. Tackling ever increasing and complex challenges, and ensuring implementation of the OAS, requires Ukraine to further identify, develop and implement effective tools and methodologies to ensure public safety.

Intelligence-Led Policing (ILP) is a modern approach, which emphasises the employment of a proactive and preventative overarching methodology, using intelligence, reliable statistics, and analysis, with effective analytical tools and credible products, to create an accurate overview of the criminal situation, identify countermeasures and ensure efficient and effective planning and decision-making. For example, a key principle of ILP is the 'need to share' – sharing information and intelligence is essential.

The clear added value of adopting all elements of ILP, is why we strongly advocate the introduction of ILP as a core model for ALL Ukrainian LEA. The importance of introducing ILP as a core model across all LEA to ensure a comprehensive approach, with actors working together using ILP to achieve common objectives, cannot be underestimated. The end goal? Reduce crime and contribute to community safety!

ПЕРЕДМОВА

Сьогодні перед правоохоронними органами України постали безпрецедентні виклики: з одного боку, треба допомагати обороняти країну від російської агресії, а з іншого – забезпечувати функціонування сектору цивільної безпеки і водночас реформувати його. В цих надзвичайно складних умовах правоохоронні органи продемонстрували виняткову стійкість і готовність не лише працювати, а й самовдосконалюватися.

Комплексний стратегічний план (КСП) реформування органів правопорядку, схвалений Президентом Зеленським у травні 2023 року, визначає такі пріоритети, як розширення та покращення міжвідомчої взаємодії і підвищення ефективності виконання органами правопорядку покладених на них функцій. Крім того, КСП передбачає забезпечення подальшого розвитку системи органів правопорядку на основі застосування ризик-орієнтованих підходів, інформаційно-аналітичної діяльності, стратегічного менеджменту та прогнозування. У документі підкреслено важливість щорічного визначення пріоритетних напрямів протидії злочинності залежно від її стану, структури, динаміки і тенденцій. Щоб долати складні виклики, яких стає дедалі більше, і забезпечити реалізацію положень КСП, Україна має шукати, розробляти і впроваджувати ефективні інструменти і методології підвищення рівня безпеки своїх громадян.

Правоохоронна діяльність, керована аналітичною розвідкою (англ. Intelligence Led Policing, або ILP) – це сучасна модель правоохоронної діяльності, заснована на застосуванні комплексного проактивно-превентивного підходу, що передбачає використання даних аналітичної розвідки, надійних статистичних даних, аналізу, ефективних аналітичних інструментів і якісних аналітичних продуктів для формування чіткої картини криміногенної ситуації, визначення заходів протидії злочинності і забезпечення ефективного й результативного планування діяльності й ухвалення рішень. Одним із ключових принципів правоохоронної діяльності, керованої аналітичною розвідкою, є need to share (англ. «необхідність ділитися даними») – обмін інформацією та розвідувальними даними має велике значення.

Оскільки комплексне застосування всіх елементів ILP має очевидні переваги, ми наполегливо рекомендуємо всім правоохоронним органам України впровадити ILP як основну модель правоохоронної роботи. Важливість такого кроку важко переоцінити, адже ILP уможливить комплексний підхід і ефективну співпрацю всіх суб'єктів задля досягнення спільних цілей. Яка кінцева мета? Мета – знизити рівень злочинності і зробити життя в громадах безпечнішим.

The European Union Advisory Mission to Ukraine (EUAM) has been advising Ukrainian LEA on ILP since 2015. As a result, LEA are working on implementing a modern threat assessment system, the Serious Organised Crime Threat Assessment, which is utilised to analyse the criminal situation ensuring prioritisation and effective use of resources. In line with the concept of ILP, the National Police of Ukraine created the Criminal Analysis Department in 2017, and the Ministry of Internal Affairs has introduced mandatory lessons in criminal analysis at MoIA universities since 2020.

In order to fully implement ILP in the NPU and across LEA, further work is needed. Complex changes to processes need to be made, e.g. intelligence gathering, evaluation and collation, as well as using the entire range of analytical methods and techniques. Increasing the use of analytical products in decision-making ensures that decisions are driven by reliable and properly analysed intelligence. In addition, the application of ILP elements must be adopted by all key players within the agencies, such as intelligence contributors, analysts and decision-makers, who should be able to rely on high quality analytical products.

EUAM contributed to co-authoring and printing this guidebook. EUAM previously also provided advisory support with the following publications:

- Police manager's handbook: ILP (2019)
- Basics of Criminal Analysis (2020)
- Tactical Criminal Analysis, Theory and Practice (2020)
- Basics of criminal analysis (2021)
- "IT in criminal analysis (practical part) (2023).

All of the mentioned guidebooks and textbooks were distributed to police units and the MoIA universities in Ukraine.

EUAM is strongly committed to continue supporting Ukrainian LEA to develop and implement ILP as the standard law enforcement model across all agencies. The clear commitment from our Ukrainian counterparts, and all involved in the production of this guidebook, is welcomed and ensures real changes in the fight against crime, and on the path to European integration.

Mayra O'Sullivan, Deputy Head of EUAM

Консультативна місія Європейського Союзу в Україні (КМЄС) з 2015 року консультує українські правоохоронні органи з питань ILP. Завдяки цій взаємодії правоохоронні органи зараз працюють над впровадженням сучасної системи оцінювання загроз серйозної та організованої злочинності (SOCTA), у якій аналіз криміногенної ситуації є основою для визначення пріоритетів та ефективного використання ресурсів. Для реалізації концепції ILP Національна поліція України 2017 року створила у своїй структурі Департамент кримінального аналізу, а Міністерство внутрішніх справ з 2020 року зробило вивчення кримінального аналізу обов'язковим у своїх вищих навчальних закладах.

Звичайно, для повноцінного впровадження ILP в НПУ та інших правоохоронних органах ще треба багато чого зробити. Є необхідність впровадження комплексних змін до робочих процесів, зокрема до процесів збирання, оцінювання та упорядкування даних, а також застосування максимально широкого спектру аналітичних методів та інструментів. Ширше використання аналітичних продуктів для ухвалення рішень підвищить якість самих рішень, адже вони ґрунтуватимуться на достовірних і належним чином проаналізованих даних. Крім того, всі ключові учасники процесу: ті, хто збирає інформацію, а також аналітики та керівники, мають сприйняти та почати застосовувати всі елементи ILP, адже для ухвалення розумних рішень потрібна високоякісна аналітика.

КМЄС виступає співавтором і спонсором друку цього посібника. Раніше КМЄС надавала консультативну підтримку в процесі підготовки таких видань:

- «Довідник керівника поліції – поліцейська діяльність, керована розвідувальною аналітикою» (2019 р.);
- «Основи кримінального аналізу» (2020 р.);
- «Тактичний кримінальний аналіз: теорія та практика» (2020 р.);
- «Основи кримінального аналізу» (2021 р.);
- «Інформаційні технології в кримінальному аналізі (практична частина)» (2023 р.).

Зазначені посібники та підручники були поширені в підрозділах поліції та вищих навчальних закладах МВС України.

КМЄС має твердий намір і надалі підтримувати українські правоохоронні органи в розвитку та впровадженні ILP як стандартної моделі правоохоронної діяльності. Дякуємо нашим українським партнерам і всім, хто долучився до підготовки цього посібника, за їхню готовність втілювати концепцію ILP в життя для впровадження реальних змін в протидію злочинності на шляху України до європейської інтеграції.

Мора О'Саллівен, заступниця голови КМЄС



English language authors are fond of the expression “May you live in interesting times”. It is often claimed to be an ancient Chinese curse, though there is no evidence to support this, and the Chinese know no such idiom. Its origins aside, it is however apt because at the time this is being written, Ukraine is going through a difficult ‘interesting time’. External threats to domestic security are challenging enough, but in times of such difficulties, domestic criminal opportunities abound as enforcement and criminal justice systems are distracted and overwhelmed. Given this pivotal moment, I’m grateful to the European Union Advisory Mission for inviting me to write this foreword, and for the Mission’s consistent comprehensive support to Ukrainian authorities in the implementation of ILP.

Intelligence-led policing had its origins during another ‘interesting time’, a huge spike in crime that was overcoming the capacities of police in many countries during the late 1980s and into the 1990s. Lacking sufficient resources and seemingly unable to stem the impact on communities, police services needed more than the slow rollout of problem-oriented policing to tackle the growth of serious, organized crime.

A landmark British report from 1993 stressed the need to use resources more effectively, increase proactive work, target prolific and serious offenders, and encourage more use of criminal informants to help police penetrate organized crime groups. Since then, intelligence-led policing (ILP) has grown to include tackling offenders who work in and around crime hotspots, addressing the spread of gangs and illicit smuggling rings, and tackling criminal social networks. The National Police of Ukraine’s guide to the implementation of the ILP philosophy into the system of criminal analysis is a direct descendent of thirty years of continuous development and progress in intelligence-led policing.

This excellent guide covers not only the theory and practice of intelligence-led policing, but also—importantly—how it can function within the National Police of Ukraine. This takes the implementation of ILP from an abstract notion to a more useful ‘how-to’. Practical implementation requires that special attention be focused on the development of intelligence gathering and processing capacities. I suspect that the biggest challenges for analysts and officers looking to develop ILP will lie in the last chapters, and especially chapter 4. Developing and creating analytical products requires an

Англомовні автори полюбляють вислів «Бодай ти жив у цікаві часи!». Багато хто вважає, що це стародавній китайський прокльон, хоча це ніде не доведено, а китайці такої фрази навіть не знають. Звідки б не походив цей вислів, він досі актуальний, адже в той час, коли я пишу ці слова, Україна переживає надзвичайно складні й, сказати б, «цікаві» часи. Зовнішні загрози національній безпеці держави – це головний, але не єдиний виклик. Справа в тім, що в складні, буремні часи з’являється також безліч кримінальних можливостей, тому що правоохоронні органи і система кримінального правосуддя, перевантажені нескінченним потоком невідкладних завдань, мають менше часу й ресурсів на протидію злочинності. У цей переломний момент історії я хочу подякувати Консультативній місії Європейського Союзу за постійну і всебічну підтримку українських органів влади у впровадженні в країні правоохоронної діяльності, керованої аналітичної розвідкою (intelligence-led policing, або скорочено ILP), а також за те, що мені випала честь написати цю передмову.

Концепція правоохоронної діяльності, керованої аналітичною розвідкою (ILP), виникла, до речі, в інші «цікаві часи», коли наприкінці 1980-х – на початку 1990-х років в багатьох країнах спостерігався величезний сплеск злочинності, з яким органи поліції не могли впоратися. Не маючи достатніх ресурсів для приборкання злочинних угруповань, від яких потерпали місцеві громади, органи поліції усвідомили, що проблему стрімкого зростання організованої злочинності неможливо подолати за допомогою самого лише проблемно-орієнтованого підходу до правоохоронної діяльності, який до того часу поступово розвивався і поширювався на теренах багатьох країн.

У Великій Британії 1993 року на тлі цих подій з’являється історичний за своїм значенням звіт, у якому наголошено на потребі використовувати ресурси більш ефективно, намагатися більше діяти на випередження («проактивний підхід»), приділяти більше уваги рецидивістам і правопорушникам, які вчиняють тяжкі й особливо небезпечні злочини, а також активніше використовувати агентурні можливості для інфільтрації в організовані злочинні групи. Концепція ILP відтоді поступово розвивалася і розросталася: зараз вона охоплює також боротьбу з правопорушниками, які вчиняють злочини в так званих кримінальних «гарячих точках» (hot spots, або місця концентрації) і поблизу них, а також боротьбу з бандами, нелегальними каналами контрабанди і злочинними соціальними мережами. Тож видання «Реалізація філософії ILP в системі кримінального аналізу Національної поліції України» можна розглядати як квінтесенцію здобутків і напрацювань у сфері ILP за останні тридцять років.

У цьому чудовому виданні охоплюються не лише теоретичні й практичні аспекти правоохоронної діяльності, керованої аналітичною розвідкою, а й також те, як цю діяльність реалізовуватиме Національна поліція України. Видання не стільки про те, що таке ILP з погляду абстрактної теорії, скільки про те, як цю модель впроваджувати й використовувати. Успішне застосування ILP залежатиме від того, чи буде зроблено акцент на

understanding of the capacities and needs of decision-makers who will—ideally—use the products to target the serious offenders who are repeatedly exploiting criminal opportunities within Ukraine. While this guide is focused on analytical development, analysts will need to work closely with decision-makers to see their efforts bear fruit. The author Terry Pratchett once wrote "The presence of those seeking the truth is infinitely to be preferred to the presence of those who think they've found it". Finding decision-makers willing to seek the truth (rather than assume they already know it), and act on good analysis, will be key to moving the National Police of Ukraine forward.

Jerry Ratcliffe, PhD

Washington, DC

December 2023

розвитку спроможності у сфері збору й опрацювання даних аналітичної розвідки (intelligence). Підозрюю, що найбільші виклики чекають на аналітиків та фахівців з ILP в останніх розділах і особливо в розділах частини 4 видання. Розроблення і створення аналітичних продуктів вимагає розуміння можливостей і потреб керівників, яким ці продукти мають допомагати ухвалювати рішення, спрямовані на осіб, які вчиняють в Україні системні, масштабні злочини. І хоча це видання призначено насамперед для розвитку аналітичної спроможності правоохоронних органів, аналітикам потрібно буде тісно співпрацювати з керівниками, відповідальними за ухвалення рішень, задля досягнення очікуваних результатів. Письменник Террі Пратчетт якось написав: «Присутність тих, хто шукає істину, незрівнянно краща за присутність тих, хто думає, що знайшов її». Саме від осіб, які прагнуть шукати істину (а не вважати, що вони її вже знають) й ухвалювати рішення на основі якісної аналітики, залежатиме розвиток і рух Національної поліції України вперед.

Джеррі Ретклiфф, доктор філософії

м. Вашингтон, округ Колумбія, США

Грудень 2023 року

ВИСЛОВЛЕННЯ ПОДЯКИ

Державний науково-дослідний інститут МВС України та Одеський державний університет внутрішніх справ засвідчують глибоку повагу та висловлюють вдячність

Консультативній місії ЄС в Україні – за багаторічну підтримку процесів реформування органів правопорядку та значний внесок щодо імплементації моделі Intelligence-led Policing в Україні, мотивацію дослідницького та освітнього потенціалу вітчизняних науковців та фахівців і безпосередню участь у виданні цієї монографії;

Департаменту кримінального аналізу Національної поліції України щодо ініціативи проведення науково-дослідної роботи за відповідним предметом дослідження та участі практичних працівників Національної поліції у розробленні окремих розділів монографії;

Джеррі РЕТКЛІФФУ *– колишньому офіцеру британської поліції, доктору філософії, професору коледжу, професору університету Темпл (Філадельфія, США)* – за наукове наставництво та фахову оцінку видання;

рецензентам:

Віктору БІЛОУСУ – *доктору юридичних наук, професору, заслуженому юристу України;*

Михайлу КОРНІЄНКУ – *доктору юридичних наук, професору, заслуженому юристу України;*

Олександру КУЛИКУ – *доктору юридичних наук, професору;*

за проявлений інтерес до нашої роботи, відверті відгуки, слушні та цінні поради;

авторському колективу, представленому видатними науковцями, практичними працівниками, експертами в галузі кримінального аналізу та поліцейської роботи, за їх внесок у дослідження, розробку монографії та безпосередню підготовку окремих розділів цього видання:

керівник проекту Олександр КОРИСТІН – доктор юридичних наук, професор, заслужений діяч науки і техніки України – *Державний науково-дослідний інститут МВС України*;

Дмитро АФОНІН – кандидат юридичних наук, доцент – *Одеський державний університет внутрішніх справ;*

Владислав БУРАНГУЛОВ – аспірант – *Одеський державний університет внутрішніх справ;*

Роман БУТКО – начальник *Департаменту кримінального аналізу НПУ;*

Олександр ВИНОГРАДОВ – кандидат психологічних наук, доцент – *Київський національний університет імені Тараса Шевченка;*

Лариса ГЕРАСИМЕНКО – кандидат юридичних наук, доцент – *Національна академія внутрішніх справ;*

Ганна ГОРБЕНКО – *Департамент комплаєнсу та фінмоніторингу OTP Bank;*

Сергій ДЕМЕДЮК – кандидат юридичних наук – *заступник секретаря Ради національної безпеки і оборони України;*

Богдан ДЕНИСЕНКО – *Консультативна місія ЄС в Україні;*

Олександр ЗАЄЦЬ – кандидат юридичних наук, доцент – *International Association of Crime Analysts;*

Карен ІСМАЙЛОВ – кандидат юридичних наук, доцент – *Департамент кіберполіції НПУ; Одеський державний університет внутрішніх справ;*

Юрій КАРДАШЕВСЬКИЙ – доктор філософії права, докторант – *Одеський державний університет внутрішніх справ;*

Микола КАРЧЕВСЬКИЙ – доктор юридичних наук, професор – *Львівський державний університет внутрішніх справ, Науково-дослідний інститут вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України;*

Грігол КАТАМАДЗЕ – кандидат юридичних наук, Надзвичайний і Повноважний Посол – *Агентство з розшуку та менеджменту активів «АРМА»;*

Максим КОРНІЄНКО – доктор юридичних наук, професор – *Одеський державний університет внутрішніх справ;*

Юрій КРУТІК – кандидат наук з державного управління – *Державна прикордонна служба України;*

Анатолій МОВЧАН – доктор юридичних наук, професор – *Львівський державний університет внутрішніх справ;*

В'ячеслав НЕКРАСОВ – кандидат юридичних наук, професор – *Збройні сили України; Національна академія внутрішніх справ;*

Дмитро ОВСЯНЮК – *Національна академія внутрішніх справ;*

Євгеній ПАНЧЕНКО – *Департамент кіберполіції НПУ;*

Вадим ПЕТРОВ – *Департамент кримінального аналізу НПУ;*

Денис ПЄФТІЄВ – *керівник Управління кримінального аналізу НПУ у 2018-2020 рр.;*

Ігор САЛЬНІКОВ – *Департамент кримінального аналізу НПУ;*

Наталія СВИРИДЮК – доктор юридичних наук, професор – *Одеський державний університет внутрішніх справ, Національна академія Служби безпеки України*;

Андрій СИВУН – *Департамент кримінального аналізу НПУ;*

Анатолій ТІМОШИН – кандидат фіз.-мат. наук, доцент – *Харківський національний університет внутрішніх справ;*

Олена ТИХОНОВА – доктор юридичних наук, професор – *Національна академія внутрішніх справ;*

Ігор ФЕДЧАК – кандидат юридичних наук, доцент – *Львівський державний університет внутрішніх справ;*

Ганна ФОРОС – кандидат юридичних наук, доцент – *Одеський державний університет внутрішніх справ;*

Андрій ХАНЬКЕВИЧ – кандидат юридичних наук, професор – *Національний юридичний університет ім. Ярослава Мудрого, Інститут підготовки юридичних кадрів для СБУ;*

Дмитро ХУДЕНКО – *керівник Департаменту кримінального аналізу НПУ у 2021-2023 рр.;*

Дмитро ШВЕЦЬ – доктор юридичних наук, доцент, заслужений працівник освіти України – *Одеський державний університет внутрішніх справ;*

Владислав ШЕНДРИК – доктор юридичних наук, професор, заслужений юрист України – *Національний юридичний університет ім. Ярослава Мудрого, Інститут підготовки юридичних кадрів для СБУ;*

Ігор ШИШКІН – *Департамент кримінального аналізу НПУ.*

Мене часто запитують: «За що ми боремося?»
Можу відповісти: «Перестанемо боротися – тоді дізнаєтесь».

Вінстон Черчилль

ВСТУП

Передумови та обґрунтування

Повноцінний розвиток Української держави неможливий без створення стійкої й ефективної системи національної безпеки, особливо в умовах воєнної агресії рф на територію країни. Важливою ланкою безпекового середовища є Національна поліція України.

Сучасні виклики й загрози у сфері внутрішньої безпеки, нові можливості вчинення злочинів, що зумовлені впливом різноманітних соціально-економічних чинників, підвищенням мобільності та міграції населення, швидкими технологічними та інформаційно-комунікаційними змінами тощо, вимагають від Національної поліції України системних еволюційних змін, адекватної та інноваційної трансформації в діяльності, фундаментальною базою яких має стати впровадження філософії «проактивної правоохоронної діяльності».

Модель поліцейської діяльності, керованої аналітичною розвідкою (Intelligence-led Policing – ILP), розроблена як відповідь на ці зростаючі проблеми, на підставі та за допомогою ILP можна переорієнтувати правоохоронну діяльність з традиційного реагування на запобігання.

Давно стало очевидним, що правоохоронна практика, зокрема, протидія злочинності потребує оновлення, інновації, оптимізації за рахунок позитивних змін саме на рівні її аналітичного забезпечення, що і реалізується в системі Національної поліції підрозділами Департаменту кримінального аналізу.

Водночас з появою сучасних інформаційних й телекомунікаційних технологій в умовах глобальної експансії злочинності, враховуючи характер, складність та обсяги кримінальних викликів, правоохоронні органи потребують принципової зміни методології та підходів, які визначають важливість використання методів аналітичної роботи не лише як інструменту збирання доказів, а також як ресурсу стратегічного менеджменту, прогнозування на основі оцінювання ризиків, підвищення спроможностей та виявлення вразливостей – упровадження повноцінних проактивних інструментів аналітичної розвідки.

Розвідувальна компонента аналітичної діяльності потребує постійного удосконалення аналітичної практики та обізнаності керівної ланки органів та підрозділів Національної поліції України щодо специфіки використання аналітичних матеріалів у процесі ухвалення управлінських та процесуальних рішень. Саме тому особливо важливим є зосередження уваги на концепціях та ключових процесах

INTRODUCTION

Background and rationale

The full development of the Ukrainian state is impossible without the creation of a sustainable and effective national security system, especially in the context of russia's military aggression against the country. The National Police of Ukraine is an important part of the security environment.

Modern challenges and threats in the field of internal security, new opportunities for committing crimes caused by the influence of various socio-economic factors, increased mobility and migration of the population, rapid technological, information and communication changes, etc. require systemic evolutionary changes from the National Police of Ukraine, adequate and innovative transformation in its activities, the fundamental basis of which should be the implementation of the philosophy of «proactive law enforcement».

The Intelligence-led Policing (ILP) model was developed as a response to these growing challenges, and based on and with the help of ILP, law enforcement can be reoriented from traditional response to prevention.

It has long been obvious that law enforcement practice, in particular, combating crime, needs to be updated, innovated, and optimized through positive changes at the level of its analytical support, which is being implemented in the National Police system by the Crime Analysis Department.

At the same time, with the emergence of modern information and telecommunication technologies in the context of global expansion of crime, reckon with the nature, complexity and volume of criminal challenges, law enforcement agencies need a fundamental change in methodology and approaches that determine the importance of using analytical methods not only as a tool for collecting evidence, but also as a resource for strategic management, forecasting based on risk assessment, increasing capabilities and identifying vulnerabilities – implementing full-fledged proactive intelligence tools.

The intelligence component of analytical activity requires continuous improvement of analytical practice and awareness of the management of the National Police of Ukraine on the specifics of using analytical materials in the process of making managerial and procedural decisions. That is why it is particularly important to focus on the concepts

поліцейської діяльності у сфері інтелектуальної аналітичної роботи, а також кращого розуміння аналітиками й, особливо, керівниками правоохоронних підрозділів нової парадигми у сфері поліцейської діяльності.

Мета та особлива роль

Підготовка цього видання розпочалася із замовлення Департаментом кримінального аналізу НПУ науково-дослідної роботи за темою щодо обґрунтування розвитку кримінального аналізу в контексті впровадження сучасної моделі поліцейської діяльності, керованої аналітичною розвідкою (Intelligence-led Policing – ILP).

ILP – не нова тема для правоохоронних органів України. За ініціативою та за підтримки Консультативної місії ЄС в Україні з 2016 року реалізуються відповідні проєкти наукового, освітнього та практичного змісту. Водночас, незважаючи на те, що відповідною фаховою спільнотою позитивно оцінюється перспектива імплементації стандартів ILP в Україні, все ж існують розбіжності щодо розуміння ILP, підходів до цієї моделі та способів її реалізації.

Принципові розбіжності вже проявляються на рівні базових знань, методологічних засад, зокрема щодо інтерпретації ключових термінів виключно англомовного походження, їх різночитання та іноді необґрунтованого україномовного використання.

Наразі, дискусійність тлумачення терміна «intelligence» в англомовному середовищі (про це зазначається в багатьох зарубіжних авторитетних джерелах) призвела до необґрунтованої української інтерпретації у контексті ILP та нав'язування й використання у професійному спілкуванні словосполучень «химерного» змісту.

Водночас, враховуючи широку палітру типології кримінального аналізу в діяльності зарубіжної поліції, склався певний тренд (і в освітніх закладах, і на практиці) необґрунтованого тлумачення, без урахування об'єктивного наукового аналізу, вітчизняних традицій та практики видів кримінального аналізу, що знову ж не корелюється зі стандартними підходами до рівнів ILP. Можливо це і є тим гальмом розвитку стратегічної компоненти в Україні!

На фоні зазначених методологічних проблем вітчизняна академічна спільнота недостатньо проявляє ініціативу щодо пошуку обґрунтованих відповідей та формування відповідної системи знань. Саме це і відчувають практичні працівники, зокрема аналітики злочинності.

Наразі монографія включає всебічне охоплення ILP, від визначення теоретичних рамок, введення ключових концепцій та основних компонентів моделі до роз'яснення принципів практичного застосування ILP, включаючи аналіз інформації, оцінку загроз, ухвалення рішень та організаційні структури.

and key processes of police activity in the field of intellectual analytical work, as well as to better understand the new paradigm in the field of police activity by analysts and, especially, by heads of law enforcement units.

Objective and added value

The preparation of this edition began with the commissioning by the Crime Analysis Department of the NPU of a research paper on the topic of justifying the development of crime analysis in the context of implementing a modern model of intelligence-led policing (ILP).

ILP is not a new topic for Ukrainian law enforcement agencies. On the initiative and with the support of the EU Advisory Mission Ukraine, relevant scientific, educational and practical projects have been implemented since 2016. At the same time, despite the fact that the relevant professional community positively assesses the prospect of implementing ILP standards in Ukraine, there are still differences in understanding ILP, approaches to this model, and ways to implement it.

Fundamental differences are already evident at the level of basic knowledge and methodological principles, in particular, in the interpretation of key terms of exclusively English origin, their misinterpretation and sometimes unjustified use in Ukrainian.

At present, the controversial interpretation of the term «intelligence» in the English-speaking environment (as noted in many foreign authoritative sources) has led to an unjustified Ukrainian interpretation in the context of ILP and the imposition and use of «bizarre» phrases in professional communication.

At the same time, given the wide range of crime analysis typology in the activities of foreign police, there is a certain tendency (both in educational institutions and in practice) of unreasonable interpretation, without taking into account objective scientific analysis, of domestic traditions and practice of types of crime analysis, which again does not correlate with standard approaches to the ILP levels. Perhaps this is the brake on the development of the strategic component in Ukraine!

Against these methodological problems' backdrop, the national academic community does not take enough initiative to find reasonable answers and form an appropriate knowledge system. This is exactly what practitioners feel, including crime analysts.

The monograph now includes a comprehensive coverage of ILP, from defining the theoretical framework, introducing key concepts and main components of the model to explaining the principles of ILP practical application, including information analysis, threat assessment, decision-making, and organizational structures.

Саме формат монографічного видання забезпечив відповідне наукове дослідження та об'єктивність в обґрунтуванні україномовного методологічного тлумачення міжнародних стандартів та відповідної практики в діяльності аналітиків правоохоронних органів.

Таким чином, метою видання є формування системних знань та стандартів, що роками розроблялися зарубіжними колегами, звісно, із врахуванням вітчизняних традицій, кращої правоохоронної практики, для практичного застосування розробниками державної політики у сфері правоохоронної діяльності, співробітниками, які відповідають за ухвалення управлінських рішень, та аналітиками правоохоронних органів, у їх зусиллях щодо підвищення професіоналізму, ефективності та інституційної спроможності органів правопорядку.

У виданні представлено низку практичних методів та інструментів аналізу злочинності, сучасних підходів аналітичного забезпечення документування воєнних злочинів та відповідного аналітичного інструментарію реалізації ILP.

Олександр КОРИСТІН

доктор юридичних наук, професор

The format of the monographic publication ensured appropriate scientific research and objectivity in substantiating the Ukrainian-language methodological interpretation of international standards and relevant practice in the activities of law enforcement analysts.

Thus, the purpose of the publication is to formulate systematic knowledge and standards that have been developed over the years by foreign colleagues, of course, taking into account national traditions and best law enforcement practices, for practical application by law enforcement policy makers, decision makers and law enforcement analysts in their efforts to improve the professionalism, efficiency and institutional capacity of law enforcement agencies.

The publication presents a number of practical methods and tools for crime analysis, modern approaches to analytical support for documenting war crimes, and relevant analytical tools for ILP implementing.

Oleksandr KORYSTIN

DSc Law, Professor

АНАЛІТИКА В БЕЗПЕКОВІЙ ДІЯЛЬНОСТІ

DOI: https://doi.org/10.36486/978-966-2310-66-5-1

Ерудиція для мене важлива. Вона свідчить про щиру інтелектуальну допитливість.

Насім Ніколас Талеб

РОЗДІЛ 1
Сутність та теоретичне осмислення феномену аналітики

Олександр Користін
Юрій Кардашевський

Аналітика – одна із загальних функцій управління різноманітними (економічними, політичними, соціальними тощо) системами, значущість якої не схильна до впливу часу і навряд чи може бути переоцінена. У тій чи іншій мірі аналітикою займаються всі, хто має відношення до управління. Природно, що суб'єкти інтелектуально-аналітичної діяльності можуть суттєво відрізнятися за видами діяльності, її масштабами, організаційно-правовими формами, цільовими установками; це накладає певний відбиток і на зміст аналітичних процедур і функцій, що виконуються особами, які приймають рішення.

Змістовний бік аналітики дуже місткий і ґрунтується на науковому знанні. Поява Аналітики симптоматично збігається з «потужним зростанням наукового знання, що все збільшується інтенсивністю та розширюється охопленням науки» [1].

і включає велику кількість концептуальних підходів, ідей, приватних аналітичних систем, кожна з яких має свої сильні та слабкі сторони. Перш за все, змістовний бік аналітики пов'язаний зі сутнісним, системно-динамічним і ресурсним аналізом, що застосовується для адекватного відображення всього різноманіття проявів об'єктів і процесів, з якими доводиться стикатися аналітику. Обґрунтованість прийнятих різними суб'єктами управлінських рішень у значній мірі визначається якістю аналітичного забезпечення, методик аналізу тощо.

Теоретичне осмислення феномена аналітики передбачає розгляд сутності, структури аналітики як наукової дисципліни, виокремлення її основних функціональних напрямів в обробці інформації, універсальні принципи роботи з інформаційним матеріалом. Також необхідно подати предметне поле аналітики, її методологію, технологію та організаційну сторону. Змістовний бік аналітики пов'язаний із сутнісним, системно-динамічним і ресурсним аналізом інформації, що відображає реальне життя. Ядром аналітики є системний аналіз інформації про предмети, явища й процеси за збереження значної частки її невизначеності. Не можна говорити про Аналітику, якщо немає об'єкта і предмета дослідження, коли взагалі немає інформації. Аналіз може реалізувати себе лише в досить розвиненому інформаційному полі. Однією з обов'язкових умов здійснення аналітичної діяльності є стан підвищеної інформаційної невизначеності щодо об'єкта дослідження.

Більшість практиків не замислюються щодо різниці, яка існує між інформаційною та аналітичною роботою. Оскільки межа між цими поняттями розмита, інформаційно-аналітична діяльність сприймається як єдине ціле, хоча насправді є сутнісна різниця.

На сьогоднішній день уміння працювати з інформацією – це запорука професіоналізму в будь-якій сфері. Робота практичного аналітика повинна полягати в отриманні та використанні інформації відповідно до заданих цілей, спираючись переважно на вміння працювати зі смисловою складовою в інформації. На цьому шляху багато перешкод – як інтелектуального, так і психологічного плану.

> *На практиці співвідношення цих сторін єдиної інформаційно-аналітичної діяльності зміщене в бік інформаційної роботи, яка зазвичай займає до 90-95 % від загального обсягу роботи. [2]*

Як правило, ускладнень з цим значно менше, ніж на етапі власне аналітичної обробки інформації. Кожен співробітник аналітичного підрозділу вміє збирати (отримувати, знаходити) інформацію, здійснювати її первинну обробку – систематизацію, класифікацію, організувати зберігання тощо.

> *Складнощі починаються тоді, коли потрібно з цієї інформації «виростити нову якість»,*

тобто отримати нові знання, прийняти ефективне управлінське рішення, написати аналітичний документ. Для цього необхідними є навички аналітичної обробки інформації і саме з цього власне починається аналітика. На рис. 1.1 показана сутнісна різниця між інформаційною та аналітичною роботою.



Рисунок 1.1. Сутнісна різниця між інформаційною та аналітичною роботою

У численних теоретичних концепціях, що мають відношення до аналітики, є сутнісне ядро і певна універсальна технологія роботи з інформаційним матеріалом. За різними зовнішніми оболонками формалізації, систематизації, моделювання та інших способів обробки інформації стоять універсальні фундаментальні принципи, які повинен знати кожен, хто зайнятий обробкою інформації.

Багато прикладних робіт аналітичного характеру піднімають проблеми, які потребують фундаментальних досліджень. Це дає можливість перевірити теоретичні висновки на практиці. Ніяка інша перевірка не є настільки переконливою, як успішне застосування теоретичних положень у справі.

Аналітика призначена для вивчення поглибленого змісту і сенсу фактів, явищ і процесів, поданні їх у вигляді теоретичної моделі, для вироблення адекватних оцінок ситуації, прогнозування, підготовки управлінських рішень.

Сутність аналітики до кінця багато хто не розуміє, навіть ті, хто мали б за своїм службовим статусом давно використовувати її на практиці.

> ***Наприклад**, у керівника у наявності є матеріали з різними даними та інформацією за профілем діяльності організації: інформаційні зведення, доповідні та службові записки, бухгалтерські документи, квартальні, піврічні та річні звіти про діяльність структурних підрозділів, плани роботи і результати перевірок, матеріали ЗМІ тощо. Цілком природно, що в цьому масиві даних інформація різного плану – від вкрай важливої до незначної, «порожньої» та тієї, що потрапила випадково. Чим вище за рангом керівник (особа, яка приймає рішення), тим суворіший відбір матеріалів, з відповідною його рівню розгляду інформацією.*
>
> *Особа, яка приймає рішення, з усього цього інформаційного багатства, що всебічно характеризує різні аспекти діяльності організації, переважно потребує остаточного сутнісного знання, яке до того, як буде викладено на папері та реалізовано в управлінському рішенні, є умовно «прихованим», непроявленим, латентним. Виявлення цього «прихованого» – сенсу, ідеї, чинників, тенденцій, закономірностей, «центрів сили», загроз, ризиків, протиріч, проблем – в різнопланові інформаційній «каші» і є головним завданням аналітика. Вся попередня робота з відбору, систематизації, класифікації даних, що надходять, переходить, нарешті, з інформаційної у, власне, аналітичну стадію.*

Саме мистецтво виявлення цих латентних сутнісних елементів, які потребують для свого виявлення спеціальних аналітичних процедур і технологій, складають глибинний зміст аналітичної роботи. На їх основі приймаються управлінські рішення, оптимальним чином розподіляються сили та засоби, запускаються нові позитивні процеси в керованих системах і зупиняються процеси, які гальмують розвиток, що стали непотрібними, блокуються загрози й знижуються ризики. Вся ця робота здійснюється у виключно креативному ключі та мало піддається формалізації.

> ***Прихованими, невиявленими, «закопаними» в товщі інформації можуть бути:***
> *ідеї;*
> *міркування;*
> *сутність;*
> *зовнішні та внутрішні чинники, що впливають на ситуацію;*
> *тенденції її розвитку;*
> *закономірності;*
> *причинно-наслідкові зв'язки;*
> *цілі дій суб'єктів;*
> *ризики;*
> *ознаки загроз;*
> *проблеми;*
> *зв'язки (прямі та зворотні), взаємозалежності;*

> *патерни;*
> *«точки зростання», «запуску» нових процесів;*
> *«центри сили», сфери їх інтересів і цілепокладання тощо.*

Аналітик, який володіє навичками системного підходу, завжди буде прагнути на основі отриманої інформації зрозуміти загальний контекст ситуації (її сегмента), внутрішню структуру системи та співвідношення цих прихованих моментів всередині неї.

> *Особливо уважно потрібно ставитися до ситуацій, коли спостерігається повторюваність характеру подій. Саме такий відтворюваний ключовий образ в синергетиці називають* ***патерном*** *подій.*

Зрозуміло, що завжди будуть особливості, виняткові обставини для кожного випадку, однак головним буде саме патерн як ключ до розуміння прихованої від нас смислової конструкції та структури системи. Системне мислення аналітика націлене на розкриття сутності явища, його закономірностей, глибинних чинників, які визначають тенденції, послідовність і характер прояву подій та розвитку їх у часі та просторі. Усе це в сукупності якраз і створює патерн.

Розпізнавання і виявлення сутності проблем вимагає знання функціональної та агрегатної структури й значень параметрів об'єкта управління за нормального його функціонування.

> *«Коли ми формулюємо проблеми або обговорюємо їх, то ми завжди тим самим формуємо певну програму і план наших дій». [3]*

Сутність будь-якої проблеми прихована в сукупності протиріч. Протиріччя можуть складатися по суті й між сутностями предметів, між сутністю та явищем, змістом і формою, необхідними й випадковими властивостями, явищами тощо. Нерідко вони являють собою переплетення багатьох форм.

Розрізняють проблеми функціонування та проблеми розвитку. Коли проблема розуміється, як розбіжність між дійсним і бажаним за відомих способів подолання цієї розбіжності, а такого роду проблеми виникають, коли цілі діяльності організації не досягнуті, такі проблеми називають проблемами функціонування.

Також проблема може розглядатися як потенційна можливість. У цьому випадку вона означає розбіжність між дійсним і бажаним за невідомих способів подолання цієї розбіжності. Найчастіше вони пов'язані з невикористанням потенціалу організації в повній мірі – це проблеми розвитку.

Розпізнавання й формулювання проблеми займає важливе місце в методології аналітичної роботи. Сама проблема визначає вибір напрямів, форм і методів дослідження, шляхів досягнення результатів. Проблема – це перешкода, протиріччя, яке несе в собі елементи нових, невідомих раніше змін. Не слід плутати поняття проблема й завдання. Рішення першої завжди вимагає творчого підходу, рішення задачі передбачає знання алгоритму її вирішення.

Розглядаючи проблему як предмет дослідження, можна виділити такі характерні її параметри: реальність, актуальність, ресурсозабезпеченість, цінність передбачуваного результату. Щоб її вирішити, необхідно її спочатку визначити, тобто «побачити» протиріччя, що виникло.

Визначення – це складна процедура, що складається з декількох фаз, основними з яких є:

- виявлення проблеми, тобто визначення її симптомів (перших ознак, сформульованих на етапі опису ситуації), що дозволяє встановити наявність проблеми як невідповідність існуючого стану справ необхідному;

- діагноз проблеми, тобто встановлення причин її виникнення; діагностика базується на зборі та аналізі інформації про фактори, які послужили причиною появи проблеми, і виділення серед них керованих, впливаючи на які можна вирішити проблему. Основним інструментом діагностики виступає причинно-наслідковий аналіз. Незважаючи на очевидність відмінностей понять «симптоми», «причини», «наслідки», у практиці управлінської діяльності досить часто вони підмінюються одне одним, що призводить не до вирішення проблеми, а до її поглиблення та тиражування.

Вирішення виявленої проблеми передбачає встановлення причинно-наслідкового ланцюга, ієрархії причин і наслідків, що веде «назад» від слідства до причини до тієї точки, в якій можна почати дію, що допомагає усунути вихідні причини. Складність і важливість аналізу у разі використання процедури причиннового ланцюга полягає в необхідності постійно фіксувати місце розташування фактів, концептуальних суджень у причинновому ланцюзі. Ясно й чітко визначити проблему означає вже почати її вирішувати. Для вирішення проблеми проводиться дослідження системи (декомпозиція, аналіз і синтез), що позбавляє проблеми.

Важливим етапом дослідження проблеми є її розпізнавання, пов'язане зі здійсненням таких операцій:

- ***виокремлення проблеми*** із загальної проблемної ситуації та її формулювання у формі та вигляді необхідному та достатньому для вирішення, що включає постановку центрального питання; фіксацію того протиріччя, яке лежить в основі проблеми, і опис можливих наслідків. Розрізняють два типи формулювання проблем: суб'єктивний і об'єктивний. Проблеми першого типу фіксують у термінах потреб цього суб'єкта управління, відображають факт їх незадоволеності. Проблеми другого типу відображають недостатність тих чи інших засобів і чинників для вирішення відповідної вихідної проблеми;

- ***побудова проблеми***, що базується на методі декомпозиції та вивченні її внутрішньої структури. Внутрішню структуру проблеми становлять такі елементи, як предмет, суб'єкт, зв'язки і мета рішення. Предмет характеризує головне протиріччя, що виникло, яке відбивається в питанні: «У чому сутність проблеми?». Об'єкт проблеми відповідає на питання: «Де виникла проблема?». Суб'єкт – конкретні особи, від яких залежить вирішення проблеми. Зв'язки характеризують обмеження і відносини з іншими проблемами. Вони відображаються в питанні: «З чим пов'язана проблема?». Мета вирішення проблеми виражається в питанні: «Для чого необхідно вирішувати проблему?»;

- ***оцінка проблеми***, яка пов'язана з виявленням умов вирішення проблеми, співвіднесення потреб і можливостей під час її вирішення, її класифікація;

- ***обґрунтування проблеми***, тобто встановлення взаємозв'язків з іншими проблемами організації.

Під час дослідження проблеми розглядається низка аспектів, що стосуються масштабу проблеми, її повторюваності, наявності часу реагування на виникнення й рішення, рівня та виду ризику, ресурсозабезпеченості, кордонів проблеми, її унікальності. Співвідношення проблемної ситуації та проблеми за обсягом змісту приблизно відповідає об'єкту й предмету дослідження під час вирішення наукових завдань.

> *Прикладна частина аналітики завжди пов'язана з вирішенням конкретних завдань у різних сферах. У першу чергу, аналітика націлена на ефективне прийняття управлінських рішень,*

а, отже, – на постійне вирішення завдань, проблем, що виникають перед управлінцем, на досягнення цілей. Вирішення завдань – це досягнення необхідних змін існуючих систем і процесів або створення нових систем і процесів із заданими властивостями. Відповідно до цього, досягнення мети – це досягнення очікуваного стану систем і процесів.

Аналітична діяльність нерозривно пов'язана з процесом інтелектуального дорослішання людства. Починаючи з античних часів, нею займалися кращі та передові уми всіх народів. Стародавні філософи, вчені Середньовіччя та епохи Відродження, енциклопедисти Нового часу, архітектори індустріального суспільства й творці новітніх інтелектуальних технологій XX століття були, перш за все, високорозвиненими самодостатніми особистостями, не схильними до стадного мислення, сподвижниками думки й Духу, стихійними або свідомими системниками, які вміють виробляти нову якість з уже наявної інформації, заглядати в майбутнє, робити прорив в нове. Знаючи ціну цим якостям, правителі та політики всіх часів прагнули звернути інтелектуальну міць цих людей на службу своїм інтересам. Чимало аналітиків піднімалося до рівня керівників держав, урядів, великих політичних або економічних структур.

Оскільки аналітика своїм походженням частково зобов'язана філософським доктринам, вона зберегла звичку спиратися на якусь теоретичну систему, з якою вона якимось чином виявляється пов'язаною. Аналітика в минулому, як і більшість протонаук, будучи справою обраних, існувала в езотеричній формі. З часом все більше професій вимагали системного мислення і зростала кількість людей, які використовували аналітику як інструмент в практичній діяльності.

Серед езотеричних коренів аналітики значне місце займає поняття традиції. За останні роки це поняття реабілітовано та знайшло позитивний сенс. Але в спекулятивно-політичних цілях його значення розмито, хоча в основному під ним мають на увазі щось стабільне й позитивне, що йде від традиційного суспільства, заснованого на сакральній релігійній традиції. Існує безліч робіт, які присвячені розкриттю ролі традиції в житті суспільства [4-11] та в яких були спроби визначити перспективи й сакралізувати деяку метатрадицію, що існує в кожній державі, в команді якої найбільш сутнісні аспекти суспільного буття. Не ставлячи завдання всерйоз розглядати ці багато в чому схоластичні та фантастичні побудови, зазначено позитивну роль ідей важливих для аналітики в цілому, що містяться в цих роботах [2]. Очевидно, що традиція – це не стільки матеріальні форми будь-якої цивілізації, а також форми її соціальної (інституційної) організації, завжди досить пластичні, рухливі, що допускають кроскультурне запозичення й перенесення. Коли ми говоримо китайська (українська, японська, британська, американська) традиція, ми маємо на увазі не лише сьогоднішній день нації, а і її досить тривалий культурно-історичний, соціально-технологічний

контекст, що має на увазі традиційні цінності, упередженості, помилки, свого роду «антиуніверсалізм», що міститься в менталітеті будь-якого народу.

Аналітика і наука, хоч і мають схожі риси, але становлять собою різні концепції, які можна розрізнити. Аналітика в деяких випадках може виступати як складовий елемент науки, а наука може слугувати джерелом для аналітики, і в обох випадках більшою чи меншою мірою вони взаємодіють.

Необхідно чітко розмежувати аналітику від близької до неї сфери – науки, з якою її часто порівнюють. Дійсно, наука й аналітика є спорідненими формами інтелектуальної активності, які об'єднують у собі безліч спільних рис: вони є одними з найскладніших проявів еволюції мислення; мають схожі методи, включно з аналізом, синтезом, використанням математики й статистики та іншими; вчені й аналітики близькі за будовою свого мислення, поглядами на світ, етичними принципами й життєвими установками, що дає змогу переходити з однієї сфери в іншу й навіть поєднувати їх у собі; наукові й аналітичні підходи можуть переплітатися, в тому числі й у вигляді наукових праць.

Попри це, існують значні відмінності між наукою та аналітикою, які не дають змоги повністю їх змішувати. Більше того,

> *аналітика, яка позбавлена наукової методології та наукових основ, залишається лише безглуздою імітацією.*

Такі наукові методи, як експеримент і спостереження, можуть не мати прямого стосунку до аналітики, але вони слугують джерелом даних для неї. Водночас у кожному серйозному науковому дослідженні завжди присутній елемент аналітики, який допомагає зрозуміти й інтерпретувати зібрані факти та дані.

> *У межах науки переважно формуються вузькі фахівці, які мають чималі знання, але спеціалізовані та в межах своєї галузі. На противагу їм, аналітики є носіями більш універсального міждисциплінарного знання, з їхнього середовища виростають методологи-концептуалісти.*

Пробний камінь будь-якої теорії, будь-якої науки – це бачення знання. Чимало вчених розглядали цю проблему й дійшли висновку, що знання завжди існує в соціальному й політичному контексті. На що вказують багато дослідників: Мішель Поль Фуко, Жак Дерріда, Юрген Хабермас та ін. Звідси виникає принципове питання про статус тих чи інших видів і форм знання, тих чи інших навчальних предметів.

Наукове знання (за ступенем проникнення в його зміст і за рівнем обґрунтованості) може виступати у формі наукового факту, наукової ідеї, наукової гіпотези та наукової теорії. Такий підхід дозволяє відійти від визначення форми існування методології науки в тому вигляді, в якому ці форми склалися: «вчення», «система поглядів», «система діяльності», «сукупність наукових положень» тощо. Вищою формою наукового знання є теорія. Теорія в більш вузькому і спеціальному значенні – вища, найрозвиненіша форма організації наукового знання, що дає цілісне уявлення про закономірності та суттєві зв'язки певної сфери – об'єкта цієї теорії.

Аналітика ж «працює» переважно з формами наукового знання, що відрізняються, скажімо, від суджень, не формально (як, наприклад, теорія або модель), а, в основному, функціонально [2]. До їх переліку відносяться проблема, ідея, принцип, припущення тощо, тобто категорії академічно актуалізовані. З формального боку це просто звичайні судження. Однак за своїми функціями в аналітичному процесі та в організації знання означені форми істотно різняться.

У Новий час виник погляд, згідно з яким справжнє знання дає тільки наука, яка спирається не тільки на математику, як вважав Платон, а й на експериментальний метод – його створив і вперше успішно застосував Галілей. Тому великі основоположники класичного природознавства Галілей і Ньютон незмінно підкреслювали: наукове знання слід чітко відрізняти від псевдонаукового, будь-якого виду. У XVIII ст. з аналізом структури й меж науки виступив І. Кант, який спробував з позицій філософії обґрунтувати наукове знання, представлене ньютонівською механікою. Він запропонував точно окреслити межі науки, тим самим відокремивши її від віри, думок, міфів та інших форм донаукового знання, а також від мистецтва, моральності, релігії та інших форм свідомості. Гегель, який підійшов до розгляду істини як діалектичного процесу руху думки, став розглядати знання в більш широкому контексті. Тому він включив до складу знання і його донаукові форми, а також сучасні форми духовної культури. Такий діалектичний підхід до знання у подальшому був сприйнятий і марксизмом. [2]

Для типологізації знання можливим є застосування найрізноманітніших підстав (критеріїв). Виділяють, наприклад, знання раціональні та ті, які виражаються емоціями, феноменалістичні та есенціаналістичні, емпіричні та теоретичні, фундаментальні та прикладні, філософські й спеціальнонаукові, природничо-наукові та гуманітарні, наукові та позанаукові тощо. Згідно з вченням

М. Полані, людині властиві два типи знання: явне, артикульоване, виражене в поняттях, логічних судженнях, теоріях й інших формах раціонального мислення, і неявне, імпліцитне, що не піддається повній рефлексії на основі людського досвіду [12]. Неявне знання не артикульовано в мові та втілено в моториці, навичках сприйнятті, практичній майстерності. Воно не допускає повної експлікації, викладу в підручниках, а передається «з рук в руки», у спілкуванні та особистих контактах дослідників. Саме ознаки такого неявного знання по великому рахунку властиві аналітиці.

На сьогодні посилюється інтерес до ірраціонального, тому що лежить за межами досяжності розуму і недоступне відомим раціональним підходам. Усе більшим є переконання в тому, що людська підсвідомість і є та глибина, звідки з'являються все нові міркування, ідеї, творіння. Взаємоперехід раціонального та ірраціонального – одна з фундаментальних підстав процесу пізнання, вкрай важлива для аналітики. Однак значення нераціональних факторів не слід перебільшувати, як це роблять прихильники ірраціоналізму [2].

Надзвичайно важливим є гуманітарне знання, воно розвиває креативне ставлення до реальності в більш широкому контексті, створюючи у свідомості цілісну картину світу. Саме воно виражає прихований якісний зв'язок між наукою та аналітикою: інформацію, отриману з досвіду або дискусії потрібно перевтілити в матеріали більш високого рівня – систематизоване знання, що в результаті глибокої обробки наявної інформації або доповнення нової з використанням специфічних методів аналітики підштовхує дослідника до більш глибокого розуміння проблемної ситуації, процесу, методу тощо. Звісно, дискурсивні науково-методологічні підстави є також важливими, та не менш важливими є *інтуїтивного рівня* креативні нестандартні підходи. Таким чином,

> *наука – це знання, приведене у систему. Аналітика є інструментом (і методом, і засобом одночасно) виявлення системних взаємозв'язків для побудови систем. Аналітика обґрунтовано може називатися науковою дисципліною з притаманною їй формалізацією наукових знань.*

З часів Платона й Аристотеля в європейській науковій традиції виразно проглядаються дві зримі тенденції, засновані на онтологічному й гносеологічному концептуальних підходах. Древніх філософів та сучасних науковців на нашій планеті завжди турбували два принципових питання: як світ влаштований і як світ пізнати?

Перша тенденція, онтологічного характеру, що відповідає на питання – «як влаштований світ?» – пов'язана з систематизацією, доведеної до межі формалізації та класифікації, які стали основними методами середньовічної богословської схоластики і, згодом, науки. Раціоналістична інтерпретація Біблії, інших артефактів культури, які пов'язані з міфотворчістю, іномовним тлумаченням, уподібненням, породило Відродження, протестантизм, новоєвропейську культуру (Декарт, Гете, Гумбольдт, Мендель, Дарвін). На цьому шляху мислителі намагалися створювати онтологічну картину світу, множинні концепції структурного устрою буття.

Друга тенденція, гносеологічна, ґрунтується на дослідженнях самої онтологічної реальності, процесів, які йдуть у самому житті та націлених на пізнання її феноменів, що ближче до прикладної науки, хоча це зовсім не обов'язково. Гносеологічний підхід спрямовано на те, як пізнати об'єкт, який методологічний інструментарій застосувати, яке операційне знання законів мислення використовувати. Гносеологія шукає нові форми, методи, способи пізнання, рефлексії світу, що динамічно розвиваються.

У сучасній фундаментальній науці, системному дослідженні достатньо обґрунтованим є застосування обох зазначених методів, проте сучасний метод наукового пізнання не може однозначно відповісти, як співвідноситься те, що ми вже достовірно знаємо, з тим, що ми знову досліджуємо.

Складність сучасного системного дослідження нерідко обумовлена багатьма причинами. Серед них зазначимо недостовірність або повну відсутність первинних емпіричних даних, приховування або свідоме спотворення інформації, а також відсутність загальновизнаних математичних, статистичних моделей і підходів (нерідко ще спеціально ретельно приховуваних в «академічних» дослідженнях), розбіжності в сутнісних інтересах (у поглядах) різних груп дослідників, шкіл, державних і приватних структур та інститутів. Бувають й інші причини.

Тому сучасна аналітика змушена задіяти дуже дієві та хитромудрі методи дослідження існуючих масивів інформації для виявлення в них прямим і непрямим шляхами її сутнісних характеристик – трендів, чинників, тенденцій, переваг, ризиків, закономірностей, погроз, зв'язків, які вкрай необхідні для розуміння проблемних ситуацій і практичного застосування в маркетингу, менеджменті, сфері безпеки, правоохоронній діяльності. Їх успішно застосовують дослідні відділи великих корпорацій у своїй аналітичній діяльності, плануванні. На цьому полі переважно буде працювати гносеологічний підхід.

Коли офіційна статистика більш-менш є достовірною і доступною, тоді метою системного аналізу проблемного поля стає вибір відповідних корелянтів (параметрів або критеріїв) для опису або передбачення ситуації.

Однак фахівцю-аналітику часто доводиться вивчати ситуацію в умовах нестачі точної інформації, у складних динамічних ситуаціях, коли аналізоване середовище з величезною кількістю в ньому суперечностей, криз, факторів і функцій об'єктів (а їх теж може бути багато), що виникають, швидко змінюється. У таких умовах старі підходи й методи нерідко не працюють, аналітик повинен не стільки спиратися на колишнє знання, скільки створювати нове.

> *Новаторів, тобто людей, які здатні генерувати нові ідеї, підходи, знання, мало - за приблизними оцінками психологів всього 5-6 % від загальної чисельності людей. Інші ж просто нездатні створювати нове. [2]*

З низки об'єктивних причин адекватне відображення й оцінка реальності вкрай ускладнена. Тому для кожного аналітика необхідним є розуміння того, що світ принципово не визначений. Системи уявлень про світ і його моделі можуть бути дуже різними. Усе залежить від системи відліку, домінуючих у свідомості суспільства й людини установок, від особистих інтелектуальних, духовних і матеріальних якостей конкретних людей. Саме ці внутрішні особистісні залежності неявного характеру позначаються на структурі менталітету, технологіях аналізу, якими озброєний конкретний аналітик, і, відповідно, зумовлюють його міркування, висновки й рішення з тієї чи іншої ситуації. З урахуванням цієї обставини стає зрозумілим, чому такими «різнокаліберними» є підходи, судження та оцінки різних експертів.

У світовій аналітичній традиції завжди присутньою була езотерика або певне ментальне сакральне ядро. Езотерична частина доволі складно піддається вербальному аналізу, але, тим не менш, реально існує. Цей культурно-історичний феномен був розповсюджений протягом усієї історії людства та у більшості культур – чи то християнство, ісламські та суфійські ордени, таємниці Ізраїлю (пророки, містики, архіви тощо). [2] Концептуальна відмінність європейської аналітичної традиції від усіх інших полягає у тому, що вона, головним чином, будувалася на раціоналізмі, що сягає своїм корінням давньогрецької культури, римського державного будівництва (римського права) та загалом поступового розвитку європейської цивілізації протягом останніх 450 років. Вона достатньо відкрита, раціональна, антропоцентрична, орієнтується на людину, її права, інтереси, цінності.

Згадуючи середньовічну аналітику, перш за все, потрібно говорити про астрологію та алхімію. Достатньо цікавою є езотерика середньовічних орденів, системні елементи й знаки-символи для посвячених у декорі готичних соборів, у символіці європейських езотеричних структур й езотеричній геральдиці. Цікавою є також «аналітика» інквізиторів на процесах відьом, теологічна софістика середньовічних європейських університетів тощо.

На межі XIX–XX сторіч у низці провідних європейських країн: Німеччині, Франції, Великій Британії – були сформовані національні культури, що дозволили екстраполювати аналітику як достатньо самостійну сферу прикладного інструментального знання у наукову дисципліну, що має певний попит. Хоча за формальними ознаками цього не сталося, тим не менш, найважливіші складові аналітики почали з'являтися. Фрагменти таких знань у вигляді концептуальних ідей, планування, у тому числі стратегічного, прогностики, дезінформації, використовувались цілеспрямовано й раніше, наприклад, банківською конторою Ротшильдів у битві при Ватерлоо (1815), німецьким Генеральним штабом (1866–1871) за часів Бісмарка, однак, у цьому випадку можемо говорити про якісну відмінність – публічну аналітику, загальнодоступну соціальну систему.

Уперше державна потреба щодо аналітики (як національного проекту, імперативу) виникла для упорядкування, раціоналізації, планування організації суспільного життя, передусім, з метою удосконалення військової державної служби, а далі – як засобу запобігання соціальному безладдю. Посилення науки, поява вчених як соціальної групи у Франції в період останніх Людовиків та Бонапарта було викликане потребами укріплення централізованої держави, армії. Мобілізаційні зусилля усіх втягнутих до I Світової війни (1914–1918) держав показали можливість й неминучість подібної мобілізації, що включала й інтелектуальні зусилля. Німеччина (меншою мірою Австро-Угорщина [3]), створила ефективну військову економіку, засновану на централізованому розподілі замовлень, сировини, робочої сили, мобілізації продовольства, транспорту й усіх інших ключових ресурсів, що принципово не змінилися й підчас II Світової війни. Мобілізаційні зусилля Великої Британії й особливо Франції були набагато меншими й майже повністю вичерпувались новими інформаційними відділами спецслужб (використання пропаганди й контрпропаганди), технічними новинками (якісний розвиток техніки). Очевидно, що до початку 30-х років XX ст. ці нові віяння лише частково мали місце у США, що відбилося в *Новому Курсі* Рузвельта, у тому числі у створенні ФБР, і частково описано в концептуальній роботі Г. Форда «Моє життя, мої досягнення» [13].

Для розуміння аналітичної сутності проявів та традиції доцільно вибудувати певну концептуальну лінію з метою виявлення пріоритетів того, що ми зіставляємо і вивчаємо – загальнокультурні традиції, релігійні кліше, масові стереотипи та соціальні інститути, те, що їх забезпечує та підтримує. У сучасному, переважно атеїстичному, суспільстві їх місце займає демократичний консенсус, позитивістський культ розуму (науки) і процедури його ефективної реалізації. Учені досліджують об'єктивні чинники, пов'язані з прогнозом і верифікацією отриманих результатів. Відповідь на питання: «А чи можна за допомогою результатів дослідження змінити реальність, прогнути її у вигідний для себе бік?» прямо все ставить на свої місця. Прагматизм очевидний і переконливий.

До числа найбільш істотних моментів, що визначають саму сутність і силу аналітичної традиції, відносять наявність смислового системного ядра, створення розгалуженої аналітичної інфраструктури збору та обробки інформації на базі сучасних інформаційних технологій, наявність визнаних авторитетів, які мають свої школи та пріоритети раціоналізму й індивідуалізму як найважливішої духовної цінності.

Аналітична традиція зберігається насамперед завдяки принципам підтримки її сутнісних елементів, що зберігають основні методи, прийоми, способи, підходи роботи зі «знанням» в цілому як культурно-історичним феноменом.

Таким чином, сутність аналітики як наукової дисципліни, перш за все, необхідно пов'язувати з методологічною та інтелектуально-технологічною сторонами діяльності, які спрямовані на вирішення завдань управління або синтезу нових знань. Саме тому обґрунтованим є визначення:

> *АНАЛІТИКА – це цілісна сукупність принципів методологічного, організаційного та технологічного забезпечення індивідуальної та колективної розумової діяльності, що дозволяє ефективно обробляти інформацію з метою виявлення в ній сутнісно-смислового ядра, вдосконалення якості наявних і придбання нових знань, а також підготовки інформаційної бази для прийняття оптимальних управлінських рішень.*

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Вернадский В.И. *Биосфера и ноосфера*. URL: http://gromada-i-misto.org/wp-content/uploads/2017/11/Vernadskiy-Biosfera_Noosfera.pdf
2. Кардашевський Ю.Р. Організаційно-правові та тактичні засади аналітичної розвідки в правоохоронній діяльності: дис. … докт. філос. у галузі права / Львівський державний університет внутрішніх справ. Львів, 2020. 217 с.
3. Користін О., Кирилюк О. Основи аналітичної розвідки в системі державної безпеки. Київ: НА СБ України. 2023. 144 с.
4. Генон Р. Кризис современного мира. URL: https://kph.ffs.npu.edu.ua/!e-book/clasik/data/guenon/01/
5. Генон Р. Царство количества и знамения времени. URL: https://readli.net/chitat-online/?b=119865&pg=1
6. Генон Р. Символы священной науки. URL: https://readli.net/chitat-online/?b=119945&pg=1
7. Элиаде М. История веры и религиозных идей. Том первый: От каменного века до элевсинских мистерий. URL: http://psylib.org.ua/books/eliad02/index.htm
8. Элиаде М. История веры и религиозных идей. Том второй: От гаутамы будды до триумфа христианства. URL: https://psylib.org.ua/books/eliad03/index.htm
9. Элиаде М. История веры и религиозных идей. Том третий: От Магомета до реформации. URL: http://psylib.org.ua/books/eliad04/index.htm
10. Эвола Ю. Традиция и Европа. URL: https://readli.net/chitat-online/?b=954196&pg=1
11. Гурджиев Г.И. Все книги: Все и вся; Беседы с учениками; Эссе и размышления о Человеке и его Учении; Последний час жизни; Закономерное разнообразие проявлений человеческой индивидуальности. URL: https://readli.net/avtor/Gurdzhiev-Georgiy-Ivanovich/
12. Полани М. Личностное знание: На пути к посткритической философии. URL: https://libarch.nmu.org.ua/handle/GenofondUA/72800
13. Форд Генри. Моя жизнь, мои достижения. URL: http://loveread.ec/contents.php?id=47569

DOI: https://doi.org/10.36486/978-966-2310-66-5-2

Адже саме відхилення від простого і звичайного висвітлює дорогу розуму у пошуках істини.

Едгар Аллан По

РОЗДІЛ 2
Суспільне призначення аналітики

Владислав Шендрик
Андрій Ханькевич

Сьогодні аналітика відіграє важливу роль у різних аспектах людського життя, надаючи цінну інформацію, покращуючи процес прийняття рішень та стимулюючи прогрес у різних сферах.

Фінансові установи використовують аналітику для оцінки ризиків, виявлення шахрайства та інвестиційних стратегій. Приватні особи використовують інструменти аналітики для управління особистими фінансами, планування бюджету та прийняття інвестиційних рішень. Додатки та платформи дають уявлення про витратні звички та фінансові цілі. Фермери використовують аналітику даних для оптимізації врожайності, ефективного управління ресурсами та прийняття обґрунтованих рішень щодо посівів. Виробничі компанії використовують аналітику для моніторингу продуктивності обладнання, прогнозування потреб у технічному обслуговуванні та оптимізації виробничих процесів. Контроль якості та виявлення дефектів покращуються завдяки аналізу даних. Енергетичні компанії використовують аналітику для оптимізації виробництва, розподілу та споживання енергії. Споживачі використовують аналітику для відстеження та зменшення споживання енергії, сприяючи зусиллям зі сталого розвитку.

Уряди використовують аналітику даних для прийняття політичних рішень, розподілу ресурсів та покращення державних послуг.

Аварійні служби використовують аналітику для більш ефективного реагування на інциденти, прогнозування тенденцій і розподілу ресурсів. Громади отримують вигоду від швидшого та ефективнішого реагування на надзвичайні ситуації.

Медичні працівники використовують аналітику даних для діагностики захворювань, прогнозування результатів лікування та персоналізації планів лікування. Організації охорони здоров'я аналізують дані про пацієнтів, щоб підвищити операційну ефективність і знизити витрати. Люди використовують пристрої та гаджети для здоров'я, щоб відстежувати свою фізичну форму, сон і загальне самопочуття. Аналітика даних допомагає людям приймати обґрунтовані рішення щодо свого здоров'я та способу життя.

Спортивні команди використовують аналітику для аналізу ефективності гравців, запобігання травмам та розробки стратегії гри. Вболівальники взаємодіють з аналітикою, щоб отримати уявлення про свої улюблені команди та гравців.

Аналітика використовується для аналізу кліматичних та екологічних даних, допомагаючи зрозуміти зміни клімату та контролювати забруднення.

Навчальні заклади використовують аналітику даних для оцінки успішності студентів, визначення сфер для покращення та вдосконалення методів навчання. Студенти та батьки можуть використовувати аналітику для вибору курсів та планування освітніх траєкторій.

Дослідники з різних дисциплін використовують аналітику для аналізу експериментальних даних, моделювання складних систем і здійснення відкриттів. Космічні агентства використовують аналітику даних для планування місій, аналізу космічних даних і відкриттів про наш всесвіт. Космічні ентузіасти взаємодіють з аналітикою, щоб досліджувати небесні явища.

Міста (середовище проживання людей) використовують аналітику даних для оптимізації транспортних потоків, зменшення споживання енергії та покращання міського планування. Мешканці отримують вигоду від покращання міських послуг та зменшення заторів. Транспортні компанії використовують аналітику для оптимізації маршрутів, зменшення споживання палива та покращання планування. Логістичні компанії аналізують дані, щоб підвищити ефективність ланцюжка поставок і знизити витрати. Авіакомпанії та готелі використовують аналітику даних для управлін-

ня бронюванням, ціноутворенням та задоволеністю клієнтів. Мандрівники отримують вигоду від персоналізованих рекомендацій щодо подорожей та покращеного досвіду бронювання.

Організації використовують аналітику, щоб приймати кращі рішення стосовно персоналу, оцінювати ефективність роботи співробітників і розробляти навчальні програми. Працівники можуть використовувати аналітику для відстеження свого кар'єрного розвитку та постановки цілей.

Компанії використовують аналітику для прийняття обґрунтованих рішень щодо розробки продуктів, маркетингу та розподілу ресурсів. Фірми, що займаються дослідженням ринку, використовують аналітику для збору та аналізу споживчих даних, допомагаючи бізнесу зрозуміти ринкові тенденції та вподобання клієнтів. Компанії використовують аналітику для оптимізації рівня запасів, зменшення дефіциту та підвищення ефективності ланцюгів поставок. Споживачі отримують вигоду від більш надійної доступності та доставки продукції та користуються продуктами та послугами, адаптованими до їхніх уподобань. Платформи соціальних мереж використовують аналітику, щоб надавати споживачам цільовий контент і рекламу. Маркетологи використовують аналітику даних для вимірювання ефективності кампаній та залучення клієнтів. Потокові платформи використовують аналітику, щоб рекомендувати користувачам контент на основі їхніх звичок перегляду. Творці контенту використовують аналітику, щоб зрозуміти вподобання аудиторії та адаптувати свій контент. Роздрібні торговці використовують дані про клієнтів для оптимізації управління запасами, цінових стратегій та покращання досвіду покупок. Платформи електронної комерції використовують аналітику для рекомендацій продуктів і персоналізованого маркетингу.

Юристи використовують аналітику для аналізу документів, прогнозування результатів справ та управління великими обсягами юридичних даних. Компанії використовують комплаєнс-аналітику для забезпечення дотримання нормативних вимог і зниження ризиків.

Технології штучного інтелекту та машинного навчання значною мірою покладаються на аналіз даних для навчання, вдосконалення моделей та прогнозування. Ці технології лежать в основі різних додатків, від голосових помічників до автономних транспортних засобів.

По суті, аналітика пронизує майже кожен аспект людського життя, надаючи цінну інформацію, оптимізуючи процеси та дозволяючи приймати більш обґрунтовані рішення. Її подальший розвиток і застосування мають потенціал стимулювати інновації та вдосконалення в широкому спектрі галузей.

Разом із тим, окремою сферою використання аналітики стоїть безпековий сектор держави. Сьогодні як ніколи важливо, щоб організації, що діють у безпековому секторі держави, приймали зважені та дієві рішення, засновані на аналітиці, яка базується на фактах.

Воєнна агресія рф на територію України, політичні та фінансово-економічні кризи, що відбуваються, показали ціну невиправданих очікувань, і сьогодні безпекові питання є актуальними у всіх галузях держави. У той час, коли державні відомства, установи та організації прагнуть безпеки в дуже нестабільні часи, дані та аналітика забезпечать їм міцний фундамент і впевненість, необхідні для досягнення успіху з мінімізованим ризиком [1].

Аналітика у безпековому секторі держави відіграє важливу роль й використовується у різних сферах.

Зокрема, у сфері національної безпеки вона сприяє виявленню та аналізу загроз з боку терористичних організацій і державних терористичних утворень, завчасно виявляє «слабкі місця» у сфері інформаційних технологій та мережевої безпеки, що може призвести до негативних наслідків, таких як втрата даних, порушення конфіденційності, пошкодження комп'ютерних систем або мереж, фінансові втрати, а також може бути спрямована на протидію кіберзлочинності або кібершпигунству. Аналітика сприяє виявленню інтересів та загроз у сфері розвідувальної активності іноземних держав, допомагає у розробці стратегій та планів захисту країни.

Результати аналітичних досліджень й аналітичні звіти є надважливими під час оцінки геополітичних ризиків, вирішення міжнародних конфліктів, налагодження дипломатичних відносин й прийняття виважених рішень у сфері зовнішньої політики та національної оборони.

У сфері громадської безпеки та цивільного захисту аналітика допомагає відповідним органам і підрозділам виявляти й розшукувати правопорушників, проводити аналіз правопорушень і злочинів під час виконання завдань оперативно-розшукової діяльності та досудового розслідування, розробляти стратегії реагування на злочини, включаючи тероризм, організовану злочинність та наркотрафік, може бути використана для виявлення кримінальних тенденцій, прогнозування надзвичайних ситуацій та планування дій в екстрених ситуаціях.

За допомогою результатів аналітичних досліджень у правоохоронців та державних фінансових установ існує можливість виявляти підозрілі фінансові операції та грошові потоки, пов'язані з

незаконною діяльністю, що може стати корисним для боротьби з відмиванням коштів та іншими фінансовими злочинами.

Аналітика відграє важливу роль у підвищенні ефективності роботи митниць, сприяючи захисту національної безпеки, економіки та громадського здоров'я. За допомогою спеціальних інструментів аналізуються дані щодо товарів, які перетинають кордон, виявляються потенційні випадки контрабанди та ймовірні напрями їх виникнення. Аналітика допомагає ідентифікувати шаблони та аномалії в переміщенні товарів, що може призвести до затримання контрабандистів, виявлення наркотиків та інших незаконних товарів.

За допомогою аналітики визначаються ризики, пов'язані з постачальниками товарів та товарами, які перетинають кордон. Аналітичні алгоритми та моделі дають можливість розробляти системи визначення оцінок рівня ризику для кожної поставки товарів, що допомагає митницям ефективно розподіляти ресурси для огляду та контролю.

У сфері захисту інтелектуальної власності (наприклад, перетин державного кордону партій контрафактної продукції) аналітика допомагає виявляти випадки порушення таких прав. Митниці мають можливості аналізувати дані про переміщення товарів та виявляти підозрілі відправлення, які містять підроблені або незаконно виготовлені товари.

Аналітичні інструменти сприяють й автоматизації деяких митних процедур, таких як, наприклад, оцінка митного зобов'язання, класифікація товарів за кодами товарної номенклатури зовнішньоекономічної діяльності, що спрощує та прискорює митний контроль та зменшує ризики помилок.

Аналітика роботи митниць також дає можливість вести моніторинг потоків товарів через кордони і виявляти тренди та шаблони у міжнародній торгівлі. Це може бути корисним для розробки державних торгових стратегій та політики.

Аналітика є потужним інструментом для підвищення рівня захисту державної інфраструктури, включаючи ідентифікацію потенційних внутрішніх і зовнішніх загроз, природних катастроф, терористичних загроз та інших небезпек. Вона допомагає зрозуміти, передбачати та своєчасно відвертати можливі загрози, збільшує ефективність державних заходів з безпеки та сприяє швидкому реагуванню на проблеми, що виникають.

У прогнозуванні надзвичайних ситуацій аналітика допомагає визначити їх можливі сценарії, що у свою чергу сприяє розробленню планів дій для управління та реагування.

У світі, де кіберзагрози стають все більш складними та виразними, аналітика допомагає виявляти та аналізувати кібератаки, знаходити вразливості і розробляти заходи для своєчасного запобігання та нейтралізації.

Ефективне управління ресурсами також не обходиться без використання можливостей аналітики. Вона допомагає раціонально розподіляти ресурси для захисту інфраструктури, ідентифікувати основні пріоритети та концентрувати зусилля на найважливіших об'єктах і системах. У цій сфері аналітика дозволяє попереджувати можливі збитки, вирішувати проблеми в ранній стадії та зменшувати витрати на реагування після подій.

Загалом, аналітика є необхідним інструментом для спільної роботи різних гілок влади у вирішенні ситуацій із внутрішніми і зовнішніми загрозами, оскільки вона допомагає створити об'єктивну основу для прийняття рішень, координувати дії та забезпечувати національну безпеку та стабільність.

> *Сьогодні ж у цифровому світі головною є не інформація, а «вміння обробляти й інтерпретувати її» [2, с. 121].*

І мова йде не тільки про наукову діяльність, а й насамперед про те, що натепер прийнято називати бізнес-аналітикою, інформаційною безпекою, а також інформаційно-аналітичним забезпеченням управлінської діяльності, в тому числі в масштабах держави [3].

Аналітика заглиблюється в сутність розвідувальних та контррозвідувальних операцій, допомагає відповідати на важливі питання та ухвалювати важливі рішення. Вона стає незамінною для юрисконсультів, економістів і фінансистів, забезпечує основу для прогнозування та планування.

У медицині вона викриває суть захворювань, а в геології та сейсмології допомагає зрозуміти природні процеси та явища.

В астрономії, математиці, фізиці, хімії, біофізиці та біохімії аналітика відіграє ключову роль, розгадуючи закони природи. Інженери-конструктори, фахівці з інформаційних технологій і багатьох інших професійних галузей знаходять в аналітиці надійного союзника в дослідженнях і вирішенні складних завдань. Цей термін, хоч і не завжди зазначається, залишається невід'ємною частиною життя багатьох фахівців, надихаючи на науковий пошук і практичні досягнення.

Аналітика, у загальноприйнятому розумінні, є об'єднуючою ланкою між збором даних, їхнім аналізом, синтезом, узагальненням і прогнозуванням, відіграючи ключову роль у процесі ефективного ухвалення рішень. Окремі фахівці розглядають аналітику як самостійну наукову дисципліну, яка наділена універсальним характером через розмаїття використовуваних методів.

Утім, сьогодні термін «аналітика» зіткнувся з надмірним уживанням і часто використовується без розбору в абсолютно різних контекстах, й навіть поза межами свого істинного змісту. Це далеко не відповідає академічним нормам. Часто «аналітикою» проголошують роздуми та їхні результати, не приділяючи належної уваги їхній якості, науковості та відповідності істинному сенсу цього терміну. Навіть окремі блогери сьогодні не соромляться називати себе «аналітиками», видають свої дослідження за аналітичні дайджести. Безліч текстів, що називаються «аналітикою», суперечать відомому принципу Ніни Річчі: «Якість понад екстравагантність», і претендують на протилежне.

Час змінив ландшафт аналітичної сфери, зруйнувавши бар'єри, які колись розмежовували наукового аналітика і поверхневого коментатора, а також кон'юнктурного публіциста. Сьогодні в науковій літературі складно знайти чіткі, що відповідають сучасності, пояснення цього поняття, за деякими винятками. Ситуація ускладнюється тим, що навіть досвідчені аналітики часто вдаються до методів, які можна охарактеризувати як кустарні та орієнтовані на споживача, що підтверджує розбіжність між методологічним підґрунтям і кінцевими результатами. Отже, необхідно переглянути поняття «аналітики» і запропонувати більш актуальні інтерпретації та пояснення.

Епоха цифрових текстів, доступних через Інтернет, викликає значну потребу в просуванні текстової аналітики та викликає інтерес до пошуку інноваційних способів інтелектуального аналізу та розуміння текстів, а також до вилучення з них знань. Можливість витягувати якісну, структуровану і машинно керовану інформацію з текстів відкриває нові перспективи для створення аналітичних інструментів, здатних виявляти знання, закладені в текстах. Розширення семантичної та онтологічної глибини текстів вводить нас у нову епоху використання інформаційних ресурсів. За допомогою текстової аналітики, ми можемо ретельніше розбиратися з фрагментованими, «зашумленими» і частково структурованими даними, перетворюючи їх на цінні елементи інтегрованого, послідовного та ефективного управління інформацією.

АНАЛІТИКА ТА ІНТЕЛЕКТУАЛЬНО-РОЗУМОВА ДІЯЛЬНІСТЬ

Для повного розуміння сутності та інструментів аналітики необхідно передусім мати чітке уявлення про природу цієї форми інтелектуальної активності, про антологію аналітики та про її взаємозв'язок з іншими пов'язаними явищами та діями. Людина володіє різноманітними здібностями для вивчення і взаємодії з навколишнім світом в усій його різноманітній повноті. Однак спроба звести інтелектуально-розумову активність до чистої аналітики є необґрунтованою. Розуміння полягає в тому, що аналітика є лише однією з форм інтелектуальної розумової діяльності, один із проявів активного пізнання. Однак далеко не кожна форма інтелектуального мислення (і, отже, людського мислення) може бути зведена до аналітичного процесу.

Аналітичний процес є чимось набагато глибшим і об'ємнішим, ніж простий розумовий аналіз. Тут прихована ідея того, що аналітика охоплює активний і комплексний метод розуміння світу, здатність формувати як експертне, так і наукове мислення. Важливо розуміти, що не кожна людина має вроджені схильності до аналізу, але з певними винятками, аналітичні навички можуть бути набуті. Це залежить від начитаності, поінформованості та широкого світогляду, які, хоч і сприяють успіху в науковій діяльності, не є заміною аналітичним здібностям.

Людський розум, як і душа, не обмежується обсягом інформації. Замість того, щоб бути заповненим різноманітними знаннями, він може стати більш містким і здатним аналізувати їх. Це протилежне уявленню про те, що надмірне навчання і накопичення знань можуть скоротити здатність до роздумів. Таким чином, *інтелектуальна спроможність людини може зростати разом зі збагаченням її знань*, і історія свідчить про те, що деякі видатні особистості минулого успішно поєднували широкі знання та визначні досягнення на суспільній арені.

АНАЛІТИКА ТА ІНТУЇЦІЯ

Вочевидь, можливо розмірковувати про різні рівні аналітичних здібностей. Виходячи з рівня кваліфікації, особистих природних задатків, навчання, досвіду, часу, виділеного на аналіз, і складності предметної області, а також ступеня винагороди і мотивації аналітика, можна говорити про сильну або слабку аналітичність. Втім, аналітику можна також розглядати як мистецтво, пов'язане з розвитком індивідуальних здібностей, і навіть талановитості, включно з онтологічним мета-баченням. Як стверджував Анрі Берґсон,

> *інтуїція, як вищий пілотаж аналітичної діяльності, є надінтелектуальною здатністю, здатною сприймати нелінійні послідовності та забезпечувати безперервний розвиток минулого в теперішньому, що переходить у майбутнє [4, с. 35-36, 47, 52].*

АНАЛІТИКА І АНАЛІЗ

У сучасному контексті, термін «аналітика» стає дедалі частіше вживаним в описі статистичного процесу та математичного аналізу даних, що охоплює виокремлення кластерів, сегментацію, оцінювання та здатність прогнозувати найімовірніші сценарії розвитку подій. Проте, важливо усвідомлювати, що аналітику не можна ототожнювати з аналізом. Вона являє собою специфічне суспільне явище, а не тільки інструмент розумової діяльності людей. Аналітика складне поліструктурне утворення, яке можна розглядати з позиції діяльного, інституціонального, організаційного, ціннісного, гносеологічного, а також технологічного підходів [4].

Аналітика є мисленнєвим процесом, спрямованим на глибше розуміння явищ і є процедурою, де досліджуваний об'єкт розкладають на його складові елементи, прагнучі дослідити їх незалежно від загального контексту [4, с. 7–8]. Отже, аналітика не обмежується лише аналізом даних як таким.

Втім, потрібно зазначити, що аналітика й аналіз, незважаючи на свою відмінність, тісно взаємопов'язані та взаємозалежні. Найчастіше розмите розуміння відмінностей між ними призводить до непорозумінь. Наприклад, інженери можуть помилково вважати, що аналітика – це виключно сфера маркетологів, тоді як самі інженери займаються тільки аналізом. Таке уявлення, хоч і має деяке коріння істинності, не відображає повної картини. Інженери також можуть виконувати аналітичну роботу, яка сприяє поліпшенню виробничих процесів і забезпеченню надійності систем.

Головна відмінність між поняттями «аналіз» і «аналітика» полягає в їхній поглибленій спрямованості.

> *«Аналіз» концентрується на розкритті змісту минулих подій і на відповіді на запит «що мало місце?». Тоді як «аналітика» глибше йде далі, прагнучі побачити коріння і розгадати мотиви, що лежать в основі минулих подій, намагаючись відповісти на запитання «чому це сталося і яка перспектива?».*

Саме прогресивна аналітика, керована даними, зібраними в реальному часі, надає можливість прогнозувати події майбутнього і здійснювати стратегічне планування. Отримані безцінні знання в галузі прогнозування виступають відправною точкою для вироблення рекомендацій і впровадження системних змін, спрямованих на мінімізацію витрат від неефективності прийнятих рішень та зниження кількості помилок [5].

СИСТЕМНІСТЬ АНАЛІТИКИ

Більшість даних набувають зовсім іншого контексту і структури, коли вони сполучаються з іншими даними і розглядаються як єдине ціле в системному підході. Руйнація структур, які пов'язують об'єкти дослідження, неминуче призводить до втрати якості дослідження [6, с. 8]. Інакше кажучи, аналітика – це процес встановлення логічних та інших зв'язків (кореляцій) між речами, явищами, порядками, відносинами і процесами.

Фрідріх Карл фон Савіньї наголошував, що

> *сутність системного підходу полягає в розумінні та відображенні внутрішнього контексту або взаємозв'язку, через який окремі юридичні концепції та норми права об'єднуються у більш високе ціле для кращого розуміння [7].*

Ці схожості часто невидимі і їх виявляння значно полегшує наше розуміння. Крім того, вони можуть бути дуже різноманітними, і що більше ми здатні виявити і простежити схожість юридичних інститутів з різних точок зору, то глибшим стає наше знання. Іноді існує ілюзія схожості, де її насправді немає, і в таких випадках завданням аналітики є виключення таких помилкових уявлень.

ПАРАМЕТР ТОЧНОСТІ В АНАЛІТИЦІ

У контексті аналітики, одним із принципових параметрів є точність.

> *Аналітик, який не приділяє увагу «чистоті» даних і працює з інформацією, переповненою «сміттям», втрачає актуальність і, часто, сенс у своїй діяльності.*

Ефективність аналітики полягає у здатності витягти значущі дані із «зашумлених» масивів інформації та вміло ними оперувати. Тому процес «очищення» даних від зайвих шарів інформаційного «шуму» є невід'ємною частиною аналітичної роботи.

Найчастіше, аналітика має справу з неповними даними і стикається з невизначеностями. У таких ситуаціях аналітики можуть вдаватися до апроксимацій, використовуючи метод заміни вихідних досліджуваних об'єктів простішими, але аналогічними їм. Такий підхід дозволяє привести дані у відповідність до запитів замовника й адаптувати їх до практичних потреб аналітики, незважаючи на те, що вихідні дані могли бути надмірно параметрично точними.

ІНСТРУМЕНТАРІЙ АНАЛІТИКИ

В інструментарії аналітика розкривається його більш глибока сутність, яка виходить далеко за межі простого експерта у вузькій галузі знань. Інтелектуальні ресурси і досвід аналітика охоплюють широкий спектр сфер і не обмежуються вузькоспеціалізованими сферами. Аналітик оперує широким спектром інтелектуальних інструментів, які дають змогу адекватно досліджувати природу явищ і процесів. Він здатний виявляти приховані явища, тенденції та закономірності в потоках первинної інформації, а також будувати прогнози і створювати обґрунтовану основу для управлінських рішень.

Інструменти аналітики складаються з різноманітного і багатогранного арсеналу, залежно від сфери застосування, предмета дослідження і поставлених завдань. Водночас в основі аналітичної роботи завжди лежать методи наукового аналізу та синтезу. На додаток до цього аналітик може вдаватися до спеціалізованих аналітичних методів, таких як системний аналіз, багатофакторний аналіз, кореляційний та регресійний аналіз тощо. Також використовуються методи узагальнення, класифікації, сценарного прогнозування, моделювання, включно зі створенням складних моделей, багатовимірного позиціонування, фреймування, аналогій та онтологічного спрощення. Цей різноманітний набір інструментів допомагає аналітику повніше і глибше досліджувати й аналізувати різні аспекти предмета його аналізу.

> *Феномен аналітики включає в себе одночасно і сам процес, і результат цієї діяльності.*

Свідченням цього може служити те, що досить часто термін «аналітика» використовується для узагальненого позначення різних інформаційних продуктів, які відображають синтезовані на основі аналізу нові або вдосконалені наявні знання. У такому контексті аналітика може розглядатися як загальне поняття, що охоплює під собою окремі документи, такі як аналітичні звіти, огляди, довідки, що, у свою чергу, конкретизують це поняття на рівні конкретних видів документів. Але ж, коли ми розглядаємо це поняття в контексті діяльнісного підходу, відбувається перетинання змісту термінів «аналітика» і «аналітична діяльність». З точки зору чіткого визначення понять, така ситуація, можливо, не є найбільш задовільною, але на практиці використання слів підтверджує, що ці поняття досить часто використовуються як взаємозамінні [3].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Davenport, T., Harris, J. & Morison, R. (2010). *Analytics at Work: Smarter Decisions, Better Results*. Boston, Mass: Harvard Business Press.
2. Dyson, Esther (1997). *Release 2.0: A design for living in the digital age*. New York: Broadway Books.
3. Мандзюк О.А. Правовий потенціал поняття «аналітика». *Актуальні проблеми держави і права*. 2020. № 84. URL: https://doi.org/10.32837/apdp.v0i84.148
4. Henri, B. (2011). *La conscience et la vie. Paris: Presses Universitaires de France*.
5. Park, D. *Analysis vs. Analytics: Past vs. Future. Eetimes*. Retrieved from https://www.eetimes.com/analysis-vs-analytics-past-vs-future/
6. Bateson, G. (1979). *Mind and Nature: A Necessary Unity*. New York: E.P. Dutton.
7. Savigny, von F.C. (1840). *System des heutigen Römischen Rechts*. (Bd. 1). Berlin: Veit.

DOI: https://doi.org/10.36486/978-966-2310-66-5-3

Не можна, мабуть, інше, як тільки горем
да бідою, довести людей до розуму.
Пантелеймон Куліш

РОЗДІЛ 3
Формування та реалізація правоохоронної політики на основі наукового передбачення

Олександр Користін

Політика як явище проникає майже в усі сфери суспільного життя. Закладені в ній зміст, принципи та цінності суттєво впливають на розвиток суспільства. Але, у свою чергу, існує і зворотний порядок, оскільки політика зумовлюється соціокультурними та геополітичними особливостями та значною мірою залежить від суб'єктів політичних відносин, особливо у період суспільних трансформацій.

Численні наукові дослідження трансформаційних процесів зосереджують увагу щодо можливого формування спроможностей управління суспільними відносинами на засадах з домінуванням не об'єктивних, а суб'єктивних чинників реалізації державної політики. Аналізуючи суспільно-політичні події в Україні періоду 2004-2007 років, Ю. Шемшученко, О. Ющик акцентують увагу на пануванні так званої «політичної доцільності» в процесі реалізації державної політики, як похідної процесу протистояння різних політичних сил за владу [1]. Науковці зауважують, що зазначене і визначає зміст політичного процесу в Україні. Водночас політика асоціюється виключно з конкретною практичною діяльністю суб'єктів політичних відносин. Втрачається наукова й інтелектуальна складова аксіологічної характеристики політики як мистецтва управління у сфері суспільно-політичного життя.

Саме тому нагальною є потреба розкриття та обґрунтування наукової уяви про правоохоронну політику, розуміння сутності цього явища, пізнання його суспільної природи, що сприятимуть посиленню впливу об'єктивних чинників на правоохоронну політику, починаючи з ключових для сучасності понять, зокрема «політики розуму» та стратегічного політичного мислення на основі прогнозування суспільно-політичних процесів й наслідків.

ПОЛІТИКА РОЗУМУ

Уся історія людства, уся історія його інтелектуального зростання пронизується дилемою: прогнозованим чи невизначеним є майбутнє. Багатьох відомих вчених осяювала думка про те, що майбутнє незбагненне. Філософ сер Карл Попер [2] виокремився оригінальністю саме в частині того, що світ засадничо, невблаганно й невиправдано непрогнозований. Розвиваючи цю ідею, Насім Ніколас Талеб [3] акцентує на тому, що наші успіхи у моделюванні (і прогнозуванні) світу знівельовано дедалі більшою складністю цього світу, зростає й роль непередбачуваного.

Але чи може людина відмовитись від передбачування майбутнього? Незважаючи на зазначене, *homo sapiens* тим і відрізняється, що усю історію людства намагається осягнути розумом майбутнє, підняти завісу й заглянути у майбутнє, хоча б недалеке. З цього приводу Платон [4] зазначав, що людина завжди прагне проникнути очима розуму в майбутнє. А Даніел Денет [5], виділяючи найбільш затребувану властивість нашого мозку, зазначає щодо здатності робити припущення про майбутнє й програвати альтернативні сценарії, а також, що наш мозок «прогностичний механізм».

Ґенеза такого намагання вдало ілюструється певною послідовністю. Від ранніх форм опанування людиною майбутнього – *міфології*, передбачення майбутнього, що пов'язувалося з розумом і діяльністю людей, а не надприродними силами – *утопії* футуроорієнтованого потенціалу людства – *фантастики*, до *наукового прогнозування* та розвитку окремого напряму – науки про майбутнє – *футурології*.

У свою чергу науково-технічний прогрес остаточно закріпив обґрунтованість необхідності наукового прогнозування, про що свідчить чимало прикладів вдалого передбачення процесів майбутнього, серед яких достатньо виділити, хоча б, ідею ноосфери, сформульованої академіком Володимиром Вернадським [6, с. 159–177], згідно якої еволюція усього живого відбувається у напрямі від менш розумних до більш розумних форм життя, тобто розумовий розвиток сам по собі є сенсом життя людини.

Найважливіші висновки ідеї ноосфери стосуються, перш за все, соціальної системи суспільства, певного виду політичного устрою (ноократії), що базується на застосуванні політики розуму, заснованої на пріоритеті людського розуму:

> *владу має той, хто знає більше та робить менше помилок, що перевіряється якістю прийняття рішень.*

Виділяючи пріоритет людського розуму, важливим залишається розуміння того, що

> *чим більшою є кількість людей, яка усвідомлює ключову роль розуму, тим якіснішим стає прийняття рішень кожною людиною.*

Ще Декарт [7] визначав розум як логічний висновок з явно сформульованих посилань. Володіючи знаннями, можна приймати достатню кількість правильних рішень. Зокрема, знаючи людську природу, можна необмежено вдосконалювати суспільні відносини, або ж створити будь-яку політичну систему.

Поряд з цим, жодна людина не знає, та й не може знати, більшу частину конкретних фактів, що визначають діяльність усієї сукупності соціальної системи суспільства. І хоча на перший погляд може здатися, що це є настільки недискусійним питання, що воно ніяким чином не потребує пояснення та особливих доказів. Але завжди існує ризик забудькуватості, тому що ті знання, якими володіє окрема людина вкрай ускладнюють намагання пояснити та з розумом вплинути на процеси, які мають місце у суспільстві, що у свою чергу різко обмежує можливості їх визначення та цільового впливу на них.

Певним чином можемо стверджувати, що більшість соціальних правил поведінки, які спрямовують наші дії, є нічим іншим як формою пристосованості щодо неможливості однієї людини свідомо враховувати усі конкретні факти, які у своїй сукупності формують соціальну систему. Саме використання величезного обсягу знань, яким не може володіти жодна окрема людина, в результаті чого усі діють в межах узгодженої структури, більша частина конструктивних факторів якої індивідуальній свідомості невідома, є відмінною ознакою розвинених цивілізацій.

> *Для забезпечення найбільшої ефективності розуму необхідним є визнання того, що можливості свідомого розуму обмежені та що необхідною є потреба у процесах іншого характеру, а саме в абстрактних концепціях, які допомагають у сприйнятті складності конкретного, чого розум людини неспроможний повною мірою охопити.*

Абстракція є незамінним інструментом, що дозволяє розуму сприймати реальність, котру не можливо пізнати остаточно. Це пов'язано з тим, що абстрактність – це характеристика усіх процесів, що визначають діяльність задовго до того, як вони втілюються в усвідомлених думках чи словах. Щоразу, коли ситуація збуджує в індивіда схильність до певної схеми реакції, присутнім є базове явище, що називається абстракцією.

Таким чином, *абстрактність – це не лише якість, певним чином характерна усім розумовим процесам, але й основа здатності людини орієнтуватися у світі, що лише частково є зрозумілим, що дає йому можливість пристосовуватись до незнання більшої частини конкретних фактів свого оточення*. Водночас головним акцентом правил, що направляють діяльність людини, є центральна роль абстрактного характеру усіх розумових процесів. За такого розуміння, абстракція не є чимось тим, що розум виводить зі сприйняття реальності, а швидше властивість категорій, якими він оперує.

> *Абстракція – це не продукт розуму, а те, що складає розум. Нам не дано діяти з повними знаннями усіх фактів, що характеризують ситуацію; нам доводиться виділяти лише певні суттєві аспекти, і ми це робимо не в результаті усвідомленого та продуманого вибору, а використовуючи механізм, що контролюється нашою свідомістю.*

Ілюзія того, що розум сам по собі здатен підказати нам, що робити, і тому усі розумні люди можуть та повинні об'єднатися навколо загальної мети, як члени певної спільноти, швидко розсіюється за намагання утілити її у практику. Щоправда, водночас не зникає бажання використовувати наш розум для перетворення усього суспільства в єдину, раціональну систему.

Використання абстракцій розширює коло явищ, котрі наш інтелект може підпорядкувати собі, але досягається це лише за рахунок обмеження здатності передбачувати наслідки нашої діяльності, зокрема, і за рахунок того, що пристосовувати світ до своїх бажань ми можемо лише у загальних рисах. Саме з цієї причини лібералізм обмежує регулювання загального порядку у суспільстві встановленням таких правил, які є необхідними для формування певного мінімуму порядку, так званого стихійного порядку, деталі якого нам не дано передбачити. Таким чином, демократичне суспільство, як основа сучасної цивілізації, є результатом зростаючої здатності людини передавати

абстрактні думки, і коли ми говоримо, що – загальним для політики розуму політичних еліт є їх розум, ми маємо на увазі здатність мислити абстрактно.

У розвиток аналізу характерних складових політики розуму сучасна політична практика засвідчує залежність ефективності та результативності планування й управління від рівня прогнозування майбутніх суспільно-політичних процесів, що, зокрема, є яскраво вираженою її складовою.

У другій половині XX ст. у науковій літературі з'явилися ґрунтовні футурологічні ідеї розвитку цивілізацій. Зокрема, заслуговує уваги концепція постіндустріального суспільства Елвіна Тоффлера [8], який зазначав, що

> *розумові здібності людини є невичерпною формою капіталу й у найближчі десятиріччя пріоритету набудуть саме знання, а отримувана завдяки їм інформація стане головною формою власності.*

За його прогнозом, політичне життя в майбутньому набуде нових характеристик: інформаційні технології сприятимуть у майбутньому створенню нової організаційної антибюрократичної структури.

Зазначене без винятків та повною мірою стосується і правоохоронної політики в державі. Політика розуму в окремо взятій сфері суспільних відносин – правоохоронній, так само потребує розвитку й набуття відповідних знань, компетентного осмислення безпекової реальності в суспільстві та розвитку абстрактного мислення.

ПОЛІТИКА НАУКОВОГО ПЕРЕДБАЧЕННЯ

Відомий американський футуролог, професор політології Френсіс Фукуяма [9] у праці «*Кінець історії і остання людина*» (1992) прогнозує, що еволюційною метою сучасного суспільства є демократичний капіталізм, як безальтернативна модель політичної та економічної організації не лише розвинених країн Заходу, а й суспільств, які прагнуть реалізуватися у протистоянні за гідність людини.

Передбачування суспільно-політичних процесів охоплює теорію, методологію й практику дослідження динаміки та перспектив розвитку найрізноманітніших процесів та явищ. І від рівня такого дослідження залежить розуміння всього спектру форм суспільно-політичного життя, особливостей функціонування політичних інститутів й механізмів, геополітичних інституцій.

Розвиток суспільства у всі історичні часи, так чи інакше, характеризувався ризиковим характером, але глибоке усвідомлення ризикогенності людської діяльності є порівняно пізнім продуктом розвитку наукової думки та буденної свідомості. Тому для більшості політиків та менеджерів, так само як і для пересічних громадян, психологічно нелегко сприймається атрибутивність ризику.

Поняття ризику як культурне новоутворення виникло в XVII сторіччі у зв'язку з азартними іграми, описуючи ймовірність появи події у поєднанні з розміром втрат та виграшів. З того часу вирахування ймовірності ризику пустило глибоке коріння в науці та практиці суспільного виробництва, опираючись на математичну теорію ймовірностей. Однак у політичній практиці поняття ризику почало виходити за контекст ймовірнісного мислення й втрачати первинний зв'язок з параметром імовірності. Конструкт ризику, який зазвичай став досить широко присутнім у політичних дебатах, має мало спільного з обрахуванням шансів. Проте він є

> *комплексним поєднанням визначення змісту певної загрози та оцінок її масштабу, ймовірності й абсолютної або відносної цінності настання чи нездійснення цієї події.*

Як свідчить практичний досвід, для більшості осіб, що приймають управлінські рішення, зокрема й у сфері правоохоронної діяльності, психологічно важко адекватно сприймати атрибутивність ризику. Особливо нерозуміння важливості зазначеного мало місце в практиці державно-управлінської діяльності за радянських часів, коли головним постулатом була притаманність ризиків лише капіталістичному суспільству через дію ринкових законів, стихійності та відсутності планування. Ментальне несприйняття феномену ризику мало місце не лише у радянських державних діячів. Американський правознавець Т. Лоуві зазначає, що *у цей же, фактично, час в американській державній політиці, попри старі традиції лібералізму, які високу цінність надавали праву на ризик, домінувала доктрина захисту від ризику й декларацій побудови у Сполучених Штатах «суспільства вільного від ризику»* [10, с. 254].

Лише з приходом до влади уряду Р. Рейгана розпочалася переоцінка проблеми ризику в політичній ідеології у бік деміфологізації ідеї «суспільства, вільного від ризику» на користь пошуку конструктивних підходів до державного управління ризиками суспільного життя [10].

Обґрунтований погляд на проблему ризику базується на усвідомленні феномену ризику, що є сталим атрибутом людської життєдіяльності, з широким спектром прояву та масштабами, що пов'язані із соціально-історичним розвитком суспільства і є певним чином віддзеркаленням його інтенсивності. Для сучасного сприйняття важливим є розуміння того, що в інформаційному суспільстві за рахунок

поширення інфогенних ризиків, посилюються характерні для індустріальної стадії суспільного розвитку соціальні ризики.

Гідденс Е. зазначає, що *жити в епоху «пізньої сучасності», під якою він, по суті, розуміє інформаційне суспільство, значить жити у світі випадковостей і ризику – незмінних супутників соціальної системи, що прагне до встановлення владарювання над природою та рефлексивного творіння історії.* З його точки зору, поняття ризику стає центральним у суспільстві, яке прощається з минулим та традиційним і відкривається для незвіданого майбутнього, а в самому суспільстві з'являється таке явище, як прагнення контролювати час і колонізувати майбутнє [11, с. 107].

У свою чергу, Штомпка П., розвиваючи погляди щодо зростання ризикогенності суспільного розвитку зазначає, що *феномен ризику набуває нових якостей, пов'язаних з виникненням нових некерованих ситуацій, які приховують загрозу не лише окремим індивідам, але й соціальним системам, і в тому числі державам, наражаючи на небезпеку мільйони людей, а то й людство в цілому*. Такі нові якості ризику вирізняють його як з об'єктивної, так і з суб'єктивної точки зору, бо не лише посилюються й урізноманітнюються фактори ризику самі по собі, але й стає більш гострим, ніж коли-небудь раніше, їх сприйняття [12].

Тобто, можемо стверджувати, що феномен ризику набуває більш універсальної форми, що несе певні загрози суспільству незалежно від етнічної чи класової приналежності. Крім того, ризики глобалізуються, торкаючись все більшої кількості людей, та розповсюджуються на все більш широкі території. З'являється все більше інституцій, які спеціально опікуються проблемою ризику або ж кладуть його в основу своєї діяльності (страхування, азартні ігри, спорт, біржі тощо). У сучасних умовах окремі несприятливі події в різних країнах і регіонах світу трансформуються в цілісну глобальну проблему – проблему виживання людства в ускладнених природних і суспільно-політичних умовах, висувають на порядок денний питання про існування глобального ризику.

У 80-х рр. XX ст. з'явилася нова соціологічна теорія сучасного суспільства (*Ульріх Бек*) [13], згідно з якою, в останній третині XX ст. людська цивілізація вступила в нову фазу свого розвитку – фазу ризику. Для індустріального суспільства характерним був розподіл цивілізаційних благ, а його еволюція супроводжувалася появою нових факторів покращення життя людини. У свою чергу, *постіндустріальне суспільство – суспільство ризику – характеризується, перш за все, розподілом загроз різного походження та обумовлених ними ризиків, появою все більше негативних чинників, що накопичуються та нерівномірно розподіляються між членами суспільства.*

> *Саме розподіл ризиків стає основною складовою цивілізаційної безпеки.*

Тотальність і всеосяжність ризику на сучасному етапі розвитку суспільства сформували підстави щодо утвердження стійкого сприйняття проблеми ризику як одного з утворюючих факторів сучасного, й особливо майбутнього, суспільства, що також набуває все більшого загальносоціального значення.

Водночас У. Бек [13] вважає, що суспільство ризику формується не стільки як національне, скільки як глобальне суспільство. Ризики характеризуються глобальним характером поширення, невідчутністю, віддаленістю, невидимістю, невизначеністю, ірраціональністю, невідомістю та складністю страхування. Особливо він акцентує увагу на тому, що політична стабільність суспільства ризику характеризується стабільністю лише у відмові від усвідомлення наслідків. Тому у своїх роботах він постійно наголошує на

> *необхідності усвідомлення ризикогенного характеру сучасного суспільного розвитку на рівні суспільства та влади.*

Ризик має місце у діяльності суб'єктів управління в ситуації невизначеності, а тому є постійним атрибутом управлінської діяльності [14]. Розуміння терміна «ризик» надзвичайно варіативне, але, в будь-якому разі, це форма поведінки суспільного суб'єкта, яка пов'язана з подоланням невизначеності й відображає ступінь досягнення очікуваного результату.

З точки зору Лумана Н., слід розмежовувати ризик і небезпеку, бо

> *небезпека є завжди, оскільки немає абсолютної надійності, а ризик має місце там, де є рішення або відмова від нього.*

Тому невизначеність майбуття слід розглядати у двох перспективах залежно від того, співвідноситься воно з прийняттям рішень чи ні, бо про ризик може йти мова лише тоді, коли існує можливість прийняття, яке може потягнути за собою шкоду. Водночас вчений наголошує, що

> *вільної від ризику поведінки не існує, як і не існує абсолютної надійності. Якщо рішення не приймається і суб'єкт утримується від дій, то все одно ризику він не уникає [15].*

Так Луман Н. вважає, що усвідомлення, оцінка ризику і прийняття ризику – проблема не лише ментальна (психологічна), але й соціальна, бо сам по собі зовнішній світ не знає ніякого ризику, оскільки йому, на відміну від людини й суспільства, невідомі ніякі очікування, цінності та калькулювання ймовірностей [15].

Розкриваючи зміст терміна «ризик», перш за все, потрібно зазначити його комплексність і полінауковість. Загальні наукові засади цього поняття мали свій розвиток в соціології, економіці, прикладній математиці, психології, девіантології тощо. В останні роки дослідження ризику набуло поширення і в юридичній та політичній науках. Особливе місце ризику відведене в безпекознавчій галузі знань та практики.

Ризик у контексті правоохоронної діяльності є корисним, бо формує базові наукові засади на основі моделі інформаційного суспільства, із врахуванням теорії безпекознавства у період постіндустріального державотворення. Реалізація державної правоохоронної політики споконвічно була складною справою і завжди була пов'язана з більшою або меншою мірою ризику. Ризик полягав щонайменше у тому, що окреслена правоохоронна політика держави може бути або зовсім не втілена в життя, або втілена лише частково.

Водночас іншим варіантом ризику може бути деформоване, викривлене, спотворене втілення в життя безпекового курсу. Реалізація правоохоронної політики може дати й результати, зворотні тим, які були сплановані її розробниками, приносити замість користі шкоду, провокувати ускладнення суспільних проблем, замість їх вирішення. Буває і так, що й повністю втілений в життя задум вищого керівництва як свої побічні або відстрочені наслідки другого, третього або ще більш віддаленого порядку породжує ще більш складні проблеми, порівняно з тою, яка була успішно розв'язана. Прикладів для ілюстрації кожного із зазначених варіантів реалізації державної правоохоронної політики можна навести багато; їх велика кількість як в історії, так і в сучасності.

Інерція подібної точки зору не переборена й сьогодні. Невдачі в реалізації правоохоронної політики суспільною думкою повністю покладаються на її розробників, а ще частіше – на виконавців. Однак декларування ризико орієнтованого характеру реалізації державної правоохоронної політики може бути спекулятивного змісту, спрямованим на прикриття дійсної несумлінності та некомпетентності. Тому важливою науковою та практичною проблемою є ідентифікація ризиків безпосередньо в реалізації державної правоохоронної політики й відмежування їх від інших причин нереалізації управлінських рішень, і в тому числі згаданих вище помилок, безвідповідальності та непрофесіоналізму.

Ризик пов'язується з діяльністю суб'єктів управління в ситуації невизначеності, з динамікою об'єкта управління і середовища, в якому він існує. Але, у будь-якому разі, ризик розглядається як постійний атрибут управлінської діяльності. Значення терміна «ризик» украй варіативне, але в будь-якому разі він пов'язаний із ситуацією невизначеності.

> *Реальності нашого часу диктують необхідність у політичних діячів та топменеджменту органів правопорядку нового рівня мислення, що передбачає адекватне сприйняття ризику і його використання як істотного компонента аналізу майбутнього.*

Управління ризиками реалізації правоохоронної політики повинно ґрунтуватися насамперед на тому, що кожен із суб'єктів прийняття рішень повинен вдаватися до прогнозування майбутніх умов її здійснення та наслідків її реалізації [16].

Водночас правоохоронна державна політика буде неефективною якщо базується на неякісному прогнозуванні, або за відсутності такого взагалі. У свою чергу, ефективність прогнозування ускладнюється хаотичністю та непродуманістю політичних та адміністративних рішень. Такий стан речей є одночасно і причиною, і наслідком багаторічної неефективності українського публічного управління.

І навіть якщо суб'єкти, що приймають управлінські рішення щиро прагнуть об'єктивно спрогнозувати майбутні умови та наслідки реалізації правоохоронної політики відповідно до принципів соціальної справедливості, за браком системи для вирішення задач ризик-менеджменту такі прогнози та й самі рішення будуть необґрунтованими та хибними. Проблема стосується фактичного браку знань. Однак наявність системи необхідних знань, не завжди є гарантом ефективності прогнозування ризиків реалізації державної правоохоронної політики.

> *Існує неоднозначний зв'язок компетентності в тій або іншій сфері зі здатністю до передбачення. Крім того, компетентність за сучасних умов необхідно поєднувати із сучасною методологією ризик-менеджменту, використовуючи відповідні методики та технологічний інструментарій.*

Причиною також є тиск поточної роботи, бюрократизація відносин, що поглинають посадову особу, не лишаючи їй достатнього часу та енергії для виважених стратегічних рішень.

Людина та суспільство можуть усувати ризик, переінтерпретовувати, витісняти його зі свідомості, ігнорувати тощо. З огляду на це, ризик можна розглядати як особливий метод пізнання та управління, що виступає як набір способів прийняття рішень.

Характерною тенденцією історичного розвитку механізмів реалізації державної політики є те, що у процесі розвитку державотворення як більш масштабнішими ставали самі інституції політичного керівництва, так і більш масштабнішим, ієрархічно багатоланковим ставав апарат державної служби, який опікувався реалізацією державної політики. Наразі потужність впливу глобальних чинників стала цілком співмірною з впливом внутрішньодержавних. Однак поки що інерція старої ментальності проявляється в тому, що, обираючи способи реалізації державної політики, виробленої на національному рівні, політичні діячі адаптували її лише до національної специфіки. Врахування ж глобального контексту покладалося лише на найвищі рівні політичного керівництва.

Процеси глобалізації рухаються внаслідок взаємодії системи глобальних, геополітичних та національних інтересів. Глобальний характер транснаціональних інтересів, збалансовує національні інтереси різних держав зокрема та світового устрою у цілому, реалізуючи концепцію протистояння глобальним викликам та ідеали справедливості. Водночас не завжди вдається відстояти саме ідеали справедливості на фоні суворих реалій геополітичної боротьби, постійного процесу переваг та врівноважень інтересів окремих країн, особливо порівнюючи інтереси країн старого світу та нових країн, що стрімко розвиваються.

Уваги потребує також і те, що під впливом глобальних процесів видозмінюються й національні інтереси, які формуються під впливом потреби виживання нації у системі цілісної глобальної структури, що, у свою чергу, формує відповідну колективну свідомість. Мають місце факти парадоксальної ситуації, коли реальні політико-правові рішення більшою мірою сприяють реалізації глобальних інтересів й певним чином провокують загрози національним інтересам. Більше того, не завжди у своїх рішеннях політики національного та місцевого рівнів усвідомлюють усі можливі загрози національним інтересам, перебуваючи під впливом привабливих глобальних процесів та тенденцій. Саме тому надзвичайно важливим є контроль, врахування та забезпечення національних інтересів в умовах глобалізації.

В епоху постіндустріального суспільства врахування ризику втрати контенту національних інтересів є надзвичайно важливою складовою політичної діяльності. Навіть патріотично налаштованому політичному діячеві в зіткненні глобальних і національних інтересів нерідко важко відстоювати інтереси власної держави через труднощі ідентифікації національних інтересів, розрізнення істинного та хибного національного інтересу. Це торкається як політиків та державних службовців, так і пересічних громадян.

Як зазначав У. Бек: «Національно-державний світопорядок фрагментує глобальні нерівності; національні норми рівності виключають глобальну нерівність; порівняння інтернаціональних нерівностей закріплює неможливість порівняння в національних рамках; перевизначення іррелевантності великих нерівностей – все це дозволяє багатим та сильним державам перекладати ризик за свої рішення на бідні країни» [13].

Окрім того, в умовах інтенсивного розвитку глобальної мережі «Інтернет» створюються можливості для інформаційної культурної агресії з боку більш розвинених інформаційних суспільств стосовно менш розвинених, що тягне за собою небезпеку втрати спільнотами й суспільствами своєї культурної самобутності та нав'язування споживацьких настанов в бізнесових інтересах вузького кола транснаціональних корпорацій. Тому причин для загострення проблеми збереження національних інтересів під тиском глобальних інтересів є досить багато. Перша з них – найбільш прикра, вона пов'язана із сумнозвісною корупцією, коли посадові особи в системі державного управління сприяють поширенню й укріпленню інтересів глобальних гравців за пряму або опосередковану винагороду, свідомо ставлячи власну користь вище патріотизму й професійного обов'язку.

З іншого боку, інколи об'єктивна позиція політичного рішення на фоні протистояння глобальних і національних інтересів є неможливою за відсутності ідентифікації національних інтересів, чіткого розуміння раціонального чи необґрунтованого національного інтересу.

Сучасні прогностичні методики повинні повною мірою бути зорієнтовані на подоланні деструктивного впливу глобалізації на внутрішній розвиток. З цього приводу доречним є зазначити необхідність застосування механізму альтернативістики. У розвинених країнах на зміну глобальним

проблемам вже приходять дослідження альтернативної цивілізації й застосування технологій та методик у XXI сторіччі.

> *Управління ризиками реалізації державної правоохоронної політики в епоху глобалізації повинно ґрунтуватися насамперед на тому, що кожен із суб'єктів політичного процесу під час формування й реалізації державної правоохоронної політики повинен вдаватися до прогнозування майбутніх умов її здійснення та наслідків її реалізації.*

Водночас слід зазначити, що прогнозування безпекових ризиків не завжди є невдалим через гносеологічні труднощі. Адже, як пересвідчує багата практика політичного керівництва, державні діячі не так вже й рідко під прикриттям декларування загальнонаціональних інтересів насправді реалізують інтереси чужі, геополітичні, власні, корпоративні, кланові, особисті й в тому числі навіть ціною завдання шкоди загальнонаціональним інтересам.

Іншими словами, невиправдана ризикованість державної політики може бути не обов'язково результатом реальних прогностичних помилок політиків та чиновників стосовно задекларованої державної політики. Реальне політичне передбачення може бути як раз досить вдалим, але прихованим від суспільства, тому що реально суперечить національним інтересам на підтримку інтересів певного клану або корпорації. Саме із врахуванням цієї особливості

> *ці процеси можуть бути як пізнавальним процесом, так і маніпулятивним, вони можуть бути як процесом пошуку оптимальності політичних рішень щодо майбутнього, так і певним приховуванням очікуваних наслідків, так би мовити, футурологічною фальсифікацією.*

Таким чином, еволюційні перетворення, що мають місце з утвердженням інформаційного суспільства, потребують упровадження науково обґрунтованої системи заходів прогнозування суспільного розвитку у будь-якій сфері життєдіяльності. Як зазначав відомий американський футуролог Ф. Фукуяма, зрушення у бік інформаційного суспільства віталося практично всіма, хто про нього писав або говорив. Всі зміни, які принесе розвиток інформаційного суспільства, розглядалися виключно як такі, що сприяють процвітанню суспільства в цілому, а також благотворні для демократії та свободи особистості [9].

На фоні суттєвих цивілізаційних змін, розвитку інформаційного суспільства та, інколи, виключно схвального його сприйняття, не завжди враховується той факт, що наслідком інформаційної революції є не лише позитивні процеси. Ф. Фукуяма одним із перших, звернув увагу і на низку негативних явищ, пов'язаних з переходом передових індустріальних країн від індустріального суспільства до інформаційного. Цей комплекс явищ він назвав «великим розривом» [9]. Перш за все це зростання злочинності, падіння народжуваності та дестабілізація сімейних і родинних зв'язків, різке зменшення довіри до суспільних інституцій та державної влади, послаблення інтенсивності міжособистісного спілкування й стійкості стосунків між громадянами тощо.

Інший, не менш відомий американський футуролог Тоффлер Е. писав про феномен футурошоку в суспільствах, охоплених інформаційною хвилею цивілізаційного розвитку. Причиною «шоку від майбутнього» є настільки різке прискорення темпів суспільних змін під впливом впровадження новітніх інформаційно-комунікаційних технологій, що адаптаційні можливості особистості, суспільства та соціальних структур виявляються недостатніми [8]. Таким чином, державне управління розвитком інформаційного суспільства повинно гуртуватися на усвідомленні того, що побічними наслідками дій, спрямованих на втілення зазначеного ідеалу, можуть бути деструктивні процеси у функціонуванні й розвитку соціуму в цілому, і це може проявлятися, в кінцевому рахунку, у зниженні економічної ефективності суспільства та його обороноздатності, посиленні соціальної напруженості й появі внутрішніх соціальних конфліктів, падінні суспільної моралі тощо [16, с. 297].

Прогнозування за умови інформаційного суспільства повинно ґрунтуватися на усвідомленні того, що побічними наслідками дій, спрямованих на втілення зазначеного ідеалу, можуть бути деструктивні процеси у функціонуванні й розвитку соціуму в цілому, і це може проявлятися, в кінцевому рахунку, у зниженні економічної ефективності суспільства та його обороноздатності, посиленні соціальної напруженості й появі внутрішніх соціальних конфліктів, падінні суспільної моралі тощо.

Саме тому, сьогоднішні прогностичні методики у сегменті безпекових відносин мають бути спрямовані на врахування синергетичних, нелінійних метаморфоз, а не лише на лінійні й врівноважені процеси. І з цього приводу для прийняття зважених та об'єктивних рішень щодо формування та реалізації державної політики нагальним є питання формування синергетичної ментальності у політичних діячів.

Новітня українська історія нерідко є відображенням однобокого бачення вітчизняною політичною елітою та зосередженням уваги лише на позитивному прогнозуванні, ідеалізуючи майбуття та не

враховуючи можливі біфуркації у бік небажаних, побічних явищ та можливого досягнення негативних наслідків або недосягнення запланованого. І за умови технологічного телекомунікаційного розвитку суспільних відносин

> *ситуація ускладнюється тим, що цінності та система знань політичної еліти формуються не на основі наукової методології, а під впливом спонтанних ініціатив, розбурханих інформаційними технологічними засобами масових комунікацій, містифікуючи реальність та створюючи соціальні міфи.*

Така ситуація спотворює сприйняття реальності політичною елітою і соціальні міфи, набуваючи додаткової сили переконання, можуть сприйматися ними як правда здорового глузду. За такої кон'юнктурної масової свідомості, яка відповідає інтересам правлячої еліти, реальні потреби переважаючої більшості людей залишаються у тіні.

> *В інформаційному суспільстві, підсиленому роллю віртуальної реальності, соціальні ілюзії захоплюють не лише політичну еліту, а й маси людей, що негативно позначається на інтелектуальній складовій реформаторських процесів.*

Українське суспільство, цивілізаційно долучене до світового інформаційного технологічного розвитку, не лише принципово змінює напрям свого розвитку, але й змушене вирішувати як теперішні завдання, так і, породжені у минулому. І відмова від цього напряму розвитку ще більшою мірою є ризикованою, а ніж стимулювання суспільного прогресу.

Сучасні виклики національній безпеці потребують системного прогнозування з питань регіональної інтеграції і дезінтеграції, з питань європейської співпраці тощо, системного розвитку політичної аналітики, зокрема, стратегічного аналізу за ключовими напрямами безпеки та суспільного розвитку. Необхідним є стратегічний аналіз у контексті європейської та євроатлантичної інтеграції, зокрема, з точки зору ризиків. Необхідністю для України є також потреба визначення співвідношення власного сценарію розвитку з глобальними, щоб можна було оцінити місце України у світі за різними сценаріями. Наразі, стратегічний прогноз, перш за все, є проективним документом, що містить певні сценарії.

Порівнюючи стан з іншими країнами, можемо констатувати, що в Україні достатньо низький рівень попиту на стратегічну аналітику. Істотним гальмом в Україні є надзвичайно слабкий рівень, порівняно з розвиненими країнами, щодо оптимізації розвитку інформаційного суспільства та надзвичайно мала підтримка власних осередків дослідження майбутнього. Наприклад, в США існують сотні так званих «фабрик думок», «мозкових центрів», асоціацій футурологів, які займаються виключно футурологічною проблематикою, діяльність яких викликає великий інтерес як у США, так і у світі.

З огляду на зазначене, українське суспільство потребує не лише ініціатив громадянського суспільства, а й державної підтримки, щодо створення власної футурологічної інфраструктури стосовно аналізу та прогнозування сценаріїв соціально-політичного та безпекового розвитку держави в умовах інформаційного суспільства.

Незважаючи на наявність відповідної методологічної бази, залишаються певні непослідовності політичних та управлінських рішень. Зокрема, це проявляється і у тому, що такі рішення у вигляді стратегій розвитку, концепцій приймаються без відповідного попереднього стратегічного аналізу. В Україні сьогодні є чинними декілька сотень такого характеру стратегій, ініційованих різними суб'єктами суспільних відносин, яким бракує попереднього аналітичного процесу дослідження. І це надзвичайно серйозне питання, особливо з точки зору відповідальності та якості. Крім того, є й інший бік цього процесу – перевантаження управлінського процесу надлишком аналітичних матеріалів. Різні департаменти мають свої аналітичні служби, що нерідко призводить до непотрібної конкуренції між різними підрозділами одного державного органу, що обумовлює елементарний хаос, паралелізм аналітичних підрозділів, недосконаліть менеджменту.

> *Сучасна політична та управлінська правоохоронна практика засвідчує залежність ефективності та результативності планування й управління від рівня прогнозування майбутніх безпекових процесів у суспільстві.*

Передбачення цих процесів охоплює теорію, методологію й практику дослідження динаміки та перспектив розвитку найрізноманітніших явищ. І від рівня такого дослідження залежить розуміння всього спектру форм суспільного життя, особливостей функціонування правоохоронних інститутів й механізмів.

З огляду на зазначене та з урахуванням сутнісного змісту політики розуму, доречним є констатувати необхідність орієнтування під час прийняття в правоохоронній сфері політичних та управлінських

рішень на науково обґрунтовані прогнози, оскільки саме вони є однією з гарантій передбачуваного розвитку конкретних подій і суспільно-політичних процесів загалом.

З цим важко не погодитись, оскільки за сучасних умов ***неспроможність прогнозувати означає неспроможність здійснювати реформи.***

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Шемшученко Ю., Ющик О. Політика, право, конституція. *Право України.* 2007. № 8. С. 6 –8.
2. Поппер Карл Раймунд. Открытое общество и его враги. Т.1. 1992. 437 с.
3. Талеб Насім Ніколас. Чорний лебідь. Про (не)ймовірне у реальному житті / пер. з англ. М. Климчука. Київ: Наш формат, 2017. 392 с.
4. Горбатенко В.П., Бутовська І.О. Політичне прогнозування. Київ: МАУП, 2005. 152 с.
5. Хофштадтер Даглас, Деннет Дениел. Глаз разума / пер. с англ. М. Эскина. URL: https://coollib.com/b/122677-daglas-r-hofshtadter-glaz-razuma/read
6. Вернадский В.И. Биосфера и ноосфера. URL: http://gromada-i-misto.org/wp-content/uploads/2017/11/Vernadskiy-Biosfera_Noosfera.pdf
7. Хайек Фридрих Август фон. Право, законодательство и свобода: Современное понимание либеральных принципов справедливости и политики. URL: https://library.khpg.org/files/docs/1456813399.pdf
8. Тоффлер Э. Метаморфозы власти. URL: https://www.gumer.info/ bibliotek_Buks/Sociolog/Toffl/index.php
9. Фукуяма Френсис. Конец истории и последний человек. URL: https://lib.misto.kiev.ua/POLITOLOG/FUKUYAMA/konec_istorii.dhtml
10. Лоуви Т. Риск и право в истории американского государства. *THESI.* 1994. № 5. С. 253–267.
11. Гидденс Э. Судьба, риск и безопасность. *THESIS*. 1994. № 5. С. 107–134.
12. Ручка А., Танчер В. Штомпка Петро // Політична енциклопедія / редкол.: Ю. Левенець (голова), Ю. Шаповал (заст. голови) та ін. Київ: Парламентське видавництво, 2011. С. 789.
13. Бек У. Общество риска. На пути к другому модерну. URL: http://socio.karazin.ua/resources/60be71e2e8e5ef7171ef10f4f60ca8a4.pdf
14. Користін О.Є., Свиридюк Н.П. Оцінювання ризиків організованої злочинності. *Наука і правоохоронна.* 2016. № 4 (34). С. 127–131.
15. Луман Н. Понятие риска. *THESIS*. 1994. № 5. С. 135–160.
16. Розвиток національної системи фінансового моніторингу / Єфименко Т.І., Гасанов С.С., Користін О.Є. та ін. Київ: ДННУ «Акад. фін. управління», 2013. 380 с.

КОНЦЕПТУАЛІЗАЦІЯ INTELLIGENCE-LED POLICING (ILP) У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

DOI: https://doi.org/10.36486/978-966-2310-66-5-4

Переконаному переконувати інших не важко.
Фрідріх Шиллер

РОЗДІЛ 4
Зміст та інтерпретація терміна «*Intelligence*» в контексті моделі *Intelligence-led Policing*

Олександр Користін
Богдан Денисенко

Перед правоохоронними органами все більш складними є сучасні виклики. Водночас у суспільстві значно зросли вимоги щодо підвищення ефективності та результативності діяльності органів правопорядку. Саме у відповідь на нові виклики сучасними розвиненими правоохоронними системами розроблена нова модель Intelligence-led Policing (далі ILP). Ця модель не тільки забезпечує сучасний підхід до ідентифікації та планування заходів протидії зростаючим транснаціональним загрозам, таким як тероризм та організована злочинність, але також застосовується до проактивного та оперативного планування за будь-яким напрямом діяльності органів правопорядку, не є винятком і загальний правоохоронний менеджмент [1; 2]. Водночас залишаються питання методологічного характеру, зокрема щодо інтерпретації терміна «intelligence» українською мовою, сприйняття його змісту в контексті зазначеної моделі, забезпечуючи тим самим об'єктивність та повноту імплементації моделі ILP в Україні.

Intelligence-led Policing – це сучасна модель, яка передбачає інкорпорування аналітичної розвідувальної функції в загальну місію правоохоронної системи. Комплексне завдання – прогнозування ризиків та вплив на дії – передбачає комбінування аналізу та процесу прийняття рішень, що створює додаткові виклики для спеціалістів розвідувальних аналітичних служб [2, с. 25]. Незважаючи на те, що ILP є викликом традиційній і домінуючій реактивній, що базується на реагуванні, поліцейській діяльності, її прийняття та привнесення у правоохоронну діяльність проактивного мислення, визначення пріоритетів і планування не змінить того факту, що поліції завжди доведеться реагувати на інциденти, пов'язані з безпекою, та вчинені злочини [1, с. 8]. ILP передбачає суттєві зміни організаційно-управлінської структури, що в межах визначеної стратегії передбачає системний збір, обмін та аналіз відповідної інформації і призначена для надання допомоги менеджменту правоохоронних органів в ухваленні обґрунтованих рішень, які формуються на реальних даних. Зазначене стосується не лише продукування стратегічних цілей, а й щоденної операційної діяльності. У цьому сенсі ILP доповнює традиційну модель правоохоронної діяльності.

> *Серед досвідчених фахівців має місце чітке розуміння того, що адекватність інтерпретації моделі та реалізація єдиної концепції ILP потребує подолання лінгвістичних проблем, оскільки термін «intelligence» у різних мовах має різне значення.*

У виданні «OSCE Guidebook Intelligence-led Policing» і робиться акцент на тому, що «*Слово intelligence зазвичай перекладається російською мовою як дані та інформація з обмеженим доступом, які мають у своєму розпорядженні служби безпеки та інші уповноважені органи, включаючи уповноважені (відповідальні) поліцейські підрозділи, тоді як англійською «intelligence» означає всі види, розроблених правоохоронними органами та їм доступних, проаналізованих даних та інформації*» [1, с. 11]. І незважаючи на запобіжне, за для уникнення «*дисгармонії*», тлумачення, що intelligence відноситься до *проаналізованих* даних та інформації, у російськомовному перекладі цього видання ОБСЄ «intelligence» хибно інтерпретується як «*оперативні дані й інформація*» [3].

Ще більш звужено, лише як «*оперативні дані*» цей термін інтерпретується у перекладі українською мовою видання Міжнародної асоціації аналітиків злочинності (*International Association of Crime Analysts, IACA*) під назвою «Exploring Crime Analysis: Readings on Essential Skills» [4].

І це не виняток, в Україні міжнародними партнерами (КМЕС, ОБСЄ) чимало зусиль докладається щодо імплементації моделі Intelligence-led Policing у діяльність органів правопорядку, але водночас

має місце різноманітність інтерпретації ключового терміна «*intelligence*» представниками органів правопорядку, яка, переважно, не відображає змісту, сутності, духу, філософії … самої моделі ILP.

Наразі термін, що передається англійським словом «intelligence», має безліч різних визначень, залежно від контексту, культур, мов і традицій (*інтелект, розум, інформація, відомості, кмітливість, розвідка, тяма* тощо). Зокрема, інтелект – це загальна здатність людини розв'язувати проблеми, вирішувати завдання, розуміти складні поняття, сприймати інформацію, мислити логічно і творчо, аналізувати, синтезувати та оцінювати інформацію, навчатися та розвиватися. Розум можна розглядати як генеральний фактор, що визначає успіх у різних сферах життя, таких як навчання, робота, спілкування, особисті відносини та інші.

На підставі літератури з'ясовано також, що слово «intelligence» використовується одночасно для визначення методології, структури, процесу і продукту. Поряд з тим, етимологічна характеристика терміна «intelligence» у контексті сутності сучасної моделі поліцейської діяльності потребує відходу від однозначного елементарного перекладу, а обґрунтовує позицію більш широкого тлумачення. Водночас *проблема інтерпретації «intelligence» у контексті ILP має місце і безпосередньо в англомовному використанні. [1]*

І прикладом тому є широка дискусія серед фахівців. М. Петерсон (Marilyn Peterson) звернула увагу на необхідності визначення терміна «intelligence» у контексті ILP, а також на важливості розуміння різниці між «intelligence» та «information». У своїй роботі «Intelligence-led Policing: The New Intelligence Architecture» [5] Петерсон обґрунтовує необхідність відмінної термінології, яка дозволяє чітко визначати різницю між різними типами даних та їхнім використанням в контексті ILP. Зокрема, вона зазначає, що

> *«Через неправильне використання слово «intelligence» означає різні речі для різних людей. Найпоширеніша помилка – вважати «intelligence» синонімом до «інформації». Інформація – це не intelligence» [5].*

Хоча, наразі, «intelligence» у найпростішому варіанті можна описати як оброблена інформація. Це має на меті передати відчуття того, що необроблена інформація повинна бути оброблена, перш ніж її можна буде інтерпретувати. Але слово «обробка» не передає жодного реального відчуття сутності чи точності. Дійсно, якщо і є ключовий елемент, якого не вистачає, в будь-якому визначенні, яке обертається навколо ідеї обробки, то це те, що intelligence вимагає високого ступеня інтерпретації, в поєднанні з деякими неминучими, виваженими припущеннями.

Незалежно від того, в якій сфері ми використовуємо «intelligence», або які теми та інтереси привертають нашу увагу, всі практичні сегменти intelligence мають такі спільні ключові елементи (виклики), що маємо враховувати [6]:

- *проблеми потрібно вирішувати;*
- *потреба в належному плануванні;*
- *дані потрібно шукати, збирати та узагальнювати;*
- *відповіді потрібно знайти.*

Ще одне загальновживане визначення, яке втілює ці ідеї, можна сформулювати на основі різних статей Короткого оксфордського словника англійської мови та інших джерел, і воно передбачає, що intelligence можна описати такими термінами [6]:

> *Intelligence – це сума того, що відомо, інтегровано з новою інформацією, а потім остаточно інтерпретовано за значенням.*

Дійсно, термін «intelligence» є досить широким і може мати різні тлумачення залежно від контексту. У правоохоронній діяльності цей термін використовується для позначення збору, аналізу та використання інформації з різних джерел з метою розкриття злочинів та запобігання злочинності.

Однак визначення та інтерпретація терміна «intelligence» у правоохоронній діяльності може викликати певні проблеми. Один з основних проблемних моментів полягає у тому, що термін «intelligence» має багато різних визначень та тлумачень у різних країнах та контекстах. Наприклад, в США під терміном «intelligence» зазвичай розуміють інформацію, яка збирається спеціальною службою, тоді як у Великій Британії під цим терміном розуміють загальну інформацію, яка збирається поліцією.

Ще однією проблемою є те, що використання терміна «intelligence» може спричиняти певні нерозуміння та непорозуміння між різними агентствами та службами, які займаються збором та обробкою

інформації. Наприклад, одна служба може вважати певну інформацію як «intelligence», тоді як інша служба може вважати її звичайною інформацією.

У дослідженнях з ILP часто зустрічається термін «intelligence», який може мати різне тлумачення і використовуватись в різних контекстах. Зокрема, він може інтерпретуватися як розвідувальна інформація про кримінальну діяльність та злочинців, яку збирає та аналізує правоохоронна система. Також «intelligence» може означати систему, яка забезпечує збір, аналіз та розповсюдження цієї інформації, а також дії правоохоронних органів, які базуються на зібраній інформації.

> *Intelligence – можливо інтерпретувати через терміни, які найчастіше в україномовному контенті використовуються у контексті моделі ILP:*
> ***аналітика, розвідка, розвідувальна аналітика, аналітична розвідка.***

Підходи до тлумачення терміна «intelligence» можуть бути різними, проте в контексті ILP важливими є такі його характеристики, як здатність збирати, аналізувати та використовувати інформацію з метою забезпечення ефективної і результативної боротьби зі злочинністю та забезпечення громадської безпеки.

АНАЛІТИКА

Наразі у контексті моделі ILP термін ***«intelligence» можна тлумачити через термін аналітика***, оскільки обидва терміни мають спільний змістовий контекст. У контексті ILP, *intelligence* як і *аналітика* також передбачає використання для збору, аналізу та інтерпретації інформації, проте з орієнтацією на розв'язання проблем правопорядку та запобігання злочинності. Таким чином, intelligence у моделі ILP можна розглядати як розвинену форму аналітики, спрямовану на досягнення певних цілей у сфері правоохоронної діяльності.

В інтерпретації терміна «intelligence» через термін «аналітика» ми можемо розуміти, що ILP базується на здатності правоохоронних органів до збору та аналізу інформації, зокрема, щоб створити детальніші профілі злочинців, оцінити загрози для громадської безпеки та визначити ефективні методи протидії злочинності тощо.

У цьому контексті «аналітика» визначається як процес перетворення різноманітної інформації в структуровану та корисну для подальшого прийняття рішень. Таким чином, intelligence у контексті ILP має на увазі не тільки збір інформації, але й її обробку та аналіз з метою забезпечення ефективного управління правоохоронною діяльністю.

Однією з позитивних ознак тлумачення терміна «intelligence» через термін «аналітика» є те, що воно зосереджується на процесі аналізу даних, інформації, що дозволяє розуміти, що це не просто збір різних даних, а їх аналіз та перетворення на корисну інформацію.

З іншого боку, негативною стороною цього тлумачення є те, що воно може зводитись до спрощення різних аспектів роботи правоохоронних органів – до лише аналітичного процесу. Це може призвести до ігнорування важливості інших аспектів, таких як людські фактори, операційна та стратегічна діяльність, комунікація, інтуїція тощо. Також

> *акцент на аналітиці може привести до переорієнтації роботи правоохоронних органів з проактивної до реактивної, що означає, що замість фокусування уваги на запобіганні вчинення злочинів, органи правопорядку будуть реагувати на вже наявні проблеми.*

Іншою негативною ознакою тлумачення терміна «intelligence» через термін «аналітика» є те, що це може призвести до зведення всієї роботи правоохоронних органів до рівня досліджень й аналітики, зменшуючи значення ролі інших складових, таких як професійна підготовка, технічні засоби, можливості та інструменти тощо. Проте, якщо використовувати термін «аналітика» як доповнення до терміна «intelligence» в контексті ILP, це може бути корисним інструментом для забезпечення точності та раціональності в прийнятті рішень у правоохоронній діяльності.

РОЗВІДКА

Термін «розвідка» у контексті правоохоронної діяльності, може використовуватися для позначення процесу збирання та аналізу інформації про певний об'єкт або ситуацію, стан, територію тощо. У цьому контексті, термін «intelligence» може тлумачитись як інформація, яка зібрана та проаналізована в рамках розвідки.

Таке тлумачення терміна «intelligence» через термін «розвідка» може мати позитивні та негативні ознаки. Серед позитивних можна назвати:

більш точне та чітке визначення терміна, що полегшує розуміння його значення;

орієнтація на збір інформації – розвідка, як й intelligence, передбачає систематичний та структурований збір інформації про можливі загрози та кримінальну активність. Наголос на процесі збирання та аналізу інформації може сприяти спрямуванню уваги на необхідності систематичного та наукового підходу до збору даних та їхнього аналізу;

термін «розвідка» може мати відтінок «шпигунства», що вказує на те, що збір інформації може відбуватися нелегальним шляхом. Це може сприяти у визначенні правових меж дій правоохоронних органів у процесі збору інформації;

спрямованість на дії у майбутньому – розвідка, як й intelligence, дозволяє отримати інформацію, яка може стати основою для прийняття рішень у майбутньому;

спрямованість на надання підтримки діяльності правоохоронних органів – розвідка, як й intelligence, може бути корисною для підтримки діяльності правоохоронних органів та забезпечення безпеки населення.

Серед негативних ознак можна назвати:

військова конотація – термін «розвідка» має переважно військову конотацію, що може призводити до сприйняття моделі ILP як «військової» та спотворювати його значення в контексті правоохоронної діяльності;

термін «розвідка» може викликати негативну реакцію в громадськості, оскільки він асоціюється зі збором інформації про людей та їхні дії;

термін «розвідка» може мати деяку незаконність, якщо збір розвідувальної інформації здійснюється з порушенням приватності та прав людини;

необхідність великих бюджетів – розвідка, як й intelligence, вимагає великих бюджетних витрат на забезпечення діяльності розвідувальних служб, що може бути важко реалізовувати для правоохоронних органів.

Таким чином, оскільки intelligence у моделі ILP відноситься до збору та аналізу інформації з різних джерел, то термін «аналітика» відображає цю ідею краще, ніж термін «розвідка». Крім того, використання терміна «аналітика» забезпечує більш точне розуміння концепції intelligence в контексті ILP та підкреслює важливість аналізу даних та інформації в управлінні правоохоронними справами.

> *У контексті моделі Intelligence-led Policing (ILP) термін «аналітика», на відміну терміна «розвідка», краще відображає зміст поняття «intelligence».*

Це пояснюється тим, що аналітика передбачає застосування різних методів та технологій для обробки та аналізу великої кількості інформації. В основі роботи аналітиків лежать методи та техніки статистичного аналізу, експертного оцінювання та прогнозування, машинного навчання, розпізнавання образів тощо. У результаті, аналітики забезпечують поліцейські служби необхідними даними та знаннями для ефективного ведення розслідувань та запобігання злочинам.

Водночас використання терміна «розвідка» може призвести до неправильного сприйняття правоохоронного органу як воєнної організації, яка провадить розвідувальні дії на військовій основі, незважаючи на інтелектуальну складову моделі ILP. Термін «розвідка», хоч і має деякий зв'язок з роботою розвідки, але може мати військовий відтінок, що не дуже відповідає специфіці ILP. Крім того, розвідка часто асоціюється зі збором інформації шляхом шпигунства або інших нелегальних методів, що може суперечити принципам законності та етики поліцейської роботи. Тому термін «аналітика» є більш точним та відповідним для тлумачення слова «intelligence» у контексті ILP.

РОЗВІДУВАЛЬНА АНАЛІТИКА

Термін «розвідувальна аналітика» також використовується в контексті розвідки та розвідувальної діяльності, де аналітики займаються збором, оцінкою розвідувальної інформації з різних джерел та аналізом. Термін «розвідувальна аналітика» зазвичай зосереджений на зборі та аналізі розвідувальної інформації, тоді як intelligence в контексті ILP охоплює ширший спектр знань, включаючи не тільки розвідувальну інформацію, а й знання про діяльність злочинних груп, закони та політику, технології, соціальні мережі та інші аспекти.

Таким чином, термін «розвідувальна аналітика» може використовуватися для пояснення деяких аспектів intelligence в контексті ILP, але він не може повністю відображати всю сутність intelligence

у цій моделі. Водночас він поєднує у собі поняття «аналітики» та «розвідки», тобто визначається як процес збору, аналізу та розуміння інформації, що отримана з різних джерел з метою прийняття рішень. З точки зору «розвідки», він охоплює велику кількість інформації, що може бути корисною для виконання завдань ILP, а з точки зору «аналітики» – відображає ключову роль, яку відіграє аналіз інформації у роботі аналітиків у контексті філософії ILP, які повинні зібрати та обробити велику кількість різноманітної інформації для продукування оптимальних рішень.

> *Отже, термін «розвідувальна аналітика» є більш точним (ніж терміни «аналітика» та «розвідка») відображенням intelligence у контексті моделі ILP, оскільки поєднує в собі ідеї розвідки та аналітики, які є ключовими складовими роботи учасників процесів ILP.*

АНАЛІТИЧНА РОЗВІДКА

Термін «аналітична розвідка» використовується для опису діяльності, яка використовує аналітичні методи для збору, обробки та інтерпретації інформації про потенційну загрозу. У контексті ILP, термін «аналітична розвідка» можна тлумачити як діяльність, яка використовує аналітичні методи для збору та обробки інформації, що стосується злочинної діяльності, з метою виявлення потенційних загроз для громадської безпеки.

> *Аналітична розвідка – це процес збору, аналізу та інтерпретації інформації з метою виявлення та оцінки потенційних загроз, визначення можливих наслідків та розробки стратегій для їх запобігання або зменшення наслідків та створення звіту або рекомендацій для прийняття рішень.*

Цей термін часто використовується у контексті безпеки та оборони, де аналітична розвідка використовується для підготовки стратегій і тактик протидії потенційним загрозам, таким як терористичні акти, кібератаки та інші форми агресії. Термін «intelligence» також використовується в контексті розвідувальної діяльності та безпеки і має аналогічне значення: це знання, які отримуються з розвідувальної діяльності та інших джерел, та які використовуються для розробки стратегій і тактик протидії потенційним загрозам.

У контексті розвідувальних служб та поліції, аналітична розвідка пов'язана з intelligence. У цьому контексті intelligence означає інформацію, отриману з різних джерел, що використовується для прийняття рішень щодо безпеки держави або боротьби зі злочинністю. Аналітична розвідка в цьому контексті використовується для аналізу розвідувальної інформації та забезпечення необхідних знань та рекомендацій для прийняття рішень.

Отже, терміни «аналітична розвідка» та «intelligence» мають багато спільного у тому сенсі, що обидва використовуються для опису процесу збору, аналізу та інтерпретації інформації з метою виявлення та оцінювання потенційних загроз. Обидва терміни використовуються у контексті безпеки та оборони, де інформація та знання про потенційні загрози можуть бути вирішальними для розробки стратегій і тактик їх запобігання або зменшення наслідків.

Звісно тлумачення терміну «intelligence» в контексті ILP через аналітичну розвідку може мати позитивні та негативні аспекти. Серед позитивних аспектів можна виділити можливість використання аналітичних методів для збору та обробки інформації, що дозволяє отримувати більш точні та детальні дані про злочинну діяльність та потенційні загрози. Також таке тлумачення підкреслює важливість використання аналітики для забезпечення безпеки громадян.

Термін «аналітична розвідка» відображає основні характеристики intelligence в контексті моделі ILP, такі як збір та аналіз інформації з метою виявлення потенційної загрози та прийняття на основі цієї інформації рішень щодо її запобігання або нейтралізації.

Однак серед негативних аспектів можна значити те, що термін «аналітична розвідка» може бути сприйнятий як надмірно військовоорієнтований та недостатньо зорієнтований на цивільну безпеку. Крім того, використання терміна «розвідка» може викликати певний рівень недовіри серед громадськості, оскільки він асоціюється з таємною та секретною діяльністю. Хоча з часом, за умови обґрунтованого, в межах права та закону, використання терміна «аналітична розвідка» можливим є уникнення проблеми тлумачення терміна «intelligence» через військовий контекст або терміна розвідки, яке може бути сприйняте як використання тільки секретної інформації.

Водночас, оскільки термін «аналітична розвідка» має глибокий зв'язок з військовою та розвідувальною діяльністю, це додатково і більш глибоко відображає специфіку діяльності служб безпеки та правоохоронних органів. Таке тлумачення intelligence дозволяє включати в себе й аспекти розвідки, такі як збір інформації про злочинців та потенційні загрози, що може бути важливою складовою успішного виконання завдань у сфері національної безпеки та правоохоронної діяльності.

З іншого боку, термін «аналітична розвідка» може бути занадто специфічним для опису всіх аспектів intelligence, що можуть бути важливими у контексті моделі ILP. Наприклад, intelligence може включати в себе аспекти профілювання поведінки, аналіз соціальних мереж та роботу з великими обсягами даних, які можуть не мати відношення до розвідувальної діяльності. Таким чином, термін «аналітична розвідка» може бути дещо обмежувальним, що може призвести до неповного тлумачення концепції intelligence в контексті ILP.

Порівнюючи безпосередньо переваги та недоліки двох термінів «розвідувальна аналітика» та «аналітична розвідка» зазначимо, що вони можуть відрізнятися за вживанням в різних організаціях та відомствах. У деяких випадках, «розвідувальна аналітика» може використовуватися більше в контексті військової розвідки, де важливіше добування та аналіз інформації з різних джерел, щоб ухвалити рішення щодо воєнних дій. У такому випадку, «аналітична розвідка» може бути більш широким терміном, що включає в себе аналіз інформації з будь-яких джерел, у тому числі військових, політичних, економічних, соціальних тощо.

Якщо ми порівняємо переваги та недоліки двох термінів «розвідувальна аналітика» та «аналітична розвідка», то можна зробити висновок, що кожен з них має свої переваги та недоліки, але обидва терміни тією чи іншою мірою можуть використовуватися для тлумачення терміна «intelligence» у контексті моделі ILP.

Розвідувальна аналітика може бути корисною в тому випадку, коли необхідно зібрати інформацію з різних джерел та зробити швидкі рішення на основі цієї інформації. Однак цей підхід може бути недостатньо глибоким та неповним, оскільки інформація може бути неповною та неперевіреною. Аналітична розвідка, з іншого боку, може дозволити більш глибокий та детальний аналіз інформації, що зібрана з різних джерел, яка дозволяє зробити більш обґрунтовані та розумні рішення. Однак цей підхід може займати більше часу та зусиль, оскільки потрібно детально проаналізувати кожне джерело та зробити висновки на основі цієї інформації.

Переваги терміна «розвідувальна аналітика» також полягають у тому, що він, можливо, більш точно відображатиме фокус на зборі інформації, процесі отримання інформації та аналізу її, який є необхідним для здійснення розвідувальної діяльності; більш зрозумілий для фахівців зі спеціальних служб. Крім того, частіше використовується в контексті правоохоронних органів та військових структур, але може бути пов'язаний зі стереотипами та негативними уявленнями про розвідувальну діяльність.

Переваги терміна «аналітична розвідка» полягають у тому, що він більш широкий та охоплює не тільки процес отримання інформації, а і її використання для прийняття рішень та планування дій. Відображає обидва аспекти процесу розвідки та аналізу, є більш загальним та універсальним терміном, що може застосовуватися в різних контекстах. Також термін «аналітична розвідка» частіше використовується в контексті інформаційних технологій та бізнесу.

Мають місце і певні недоліки терміна «аналітична розвідка»: може бути менш зрозумілим для фахівців зі спеціальних служб; може створювати сприйняття, що обидва аспекти розвідки та аналізу є рівнозначними, тоді як розвідувальна діяльність може мати більшу або меншу вагу, залежно від контексту.

Кожен з підходів має свої переваги та недоліки, тому важко однозначно визначити, який із них найбільше відображає значення intelligence в контексті ILP. Однак можна зробити висновок, що терміни «розвідувальна аналітика» та «аналітична розвідка» є більш точними і більш повно відображають сутність intelligence у контексті ILP, оскільки поєднують у собі характеристики обох попередніх підходів «*аналітики*» і «*розвідки*».

> *За складності, багатогранності, різного в традиційному вимірі сприйняттю у суспільстві термін «аналітична розвідка» найбільш точно відображає значення «intelligence» у контексті ILP, а тому достатньо обґрунтованою є україномовна інтерпретація Intelligence-led Policing як* ***«Правоохоронна діяльність, керована аналітичною розвідкою».***

Це тлумачення дозволяє поєднувати ключові характеристики intelligence, такі як збір та аналіз інформації, з процесом розвідки, що передбачає збір, аналіз та оцінку інформації з метою надання рекомендацій. Інформація та знання про потенційні загрози можуть бути вирішальними для розробки стратегій і тактик їх запобігання або зменшення наслідків тим самим, вирішуючи завдання проактивності нової моделі. Крім того, це тлумачення підкреслює роль аналітичної складової в процесі розвідки, що є важливим аспектом в контексті ILP.

> *Термін «аналітична розвідка» найбільше відповідає сутності та значенню терміна intelligence в контексті ILP. Він поєднує в собі ключові характеристики, які мають значення для збору, аналізу та використання інформації для прийняття рішень у правоохоронній діяльності. Термін «аналітична розвідка» акцентує увагу на аналізі та обробці даних, що відповідає головній задачі intelligence у контексті ILP – збору, аналізу та використанню інформації з метою досягнення цілей правоохоронної діяльності, вирішенню комплексного завдання, що передбачає комбінування аналізу та процесу прийняття рішень, прогнозування ризиків та впливу на управлінську діяльність.*

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *OSCE Guidebook Intelligence-Led Policing* (2017). TNTD/SPMU Publication. Series Vol. 13. Vienna.
2. Користін О.Є., Пефтієв Д.О., Пеньков С.В., Некрасов В.А. *Довідник керівника поліції - поліцейська діяльність, керована розвідувальною аналітикою / ILP*. Київ: «Видавництво Людмила», 2019. 120 с.
3. Руководство ОБСЕ по полицейской деятельности на основе оперативных данных и информации, Вена: ОБСЕ, 2017. URL: https://www.osce.org/files/f/documents/a/9/357211.pdf.
4. *Exploring Crime Analysis: Readings on Essential Skills* (2017). IACA: Kansas.
5. Marilyn, Peterson (2005). *Intelligence-Led Policing: The New Intelligence Architecture*. Washington, DC: U.S. Department of Justice.
6. Don McDowell (2009). *Strategic Intelligence: A handbook for practitioners, managers, and users*. Plymouth, UK: The scarecrow press, Inc.

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

Намагайся знати все про щось і щось про все.
Генрі Пітер Брум

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

Олександр Користін
Ігор Федчак
Владислав Бурангулов

Традиційна поліцейська діяльність є найбільш відомою правоохоронною моделлю і залишається стандартним стилем правоохоронної діяльності. Це стосується реактивного й інцидентного стилю, за якого поліцейські більшою мірою тільки реагують відповідним чином на злочин і вимогу надання сервісних послуг. Відповіді на дзвінки, прийом заяв, патрулювання в громадських місцях, створюючи видимість присутності поліції, є сутністю традиційної поліцейської діяльності. Кримінальний аналіз в межах традиційної моделі реалізує свої функції переважно щодо розкриття злочинів, які вчиняються або вчинені в минулому.

Водночас новітня історія вказує на розвиток та системні зміни правоохоронної діяльності, яка переживає період значних змін як в оперативній тактиці, так і в організаційних структурах. Упроваджуються нові ідеї щодо скорочення злочинності й зміни стратегій короткострокової та довгострокової політики.

> *Сучасна правоохоронна діяльність є комплексною динамічною системою, що постійно змінюється та розвивається, балансуючи між різноманітними загрозами безпекового характеру, своєчасно реагуючи на них, забезпечуючи необхідний рівень громадської безпеки та протидії злочинності.*

Новітні виклики потребують формування відповідних інституційних спроможностей, належної реалізації правоохоронних функцій, зокрема, системного виявлення та розслідування кримінальних правопорушень, ефективного документування злочинної діяльності, якісного проведення гласних та негласних слідчих розшукових дій, фахового виконання завдань кримінальної розвідки, цільового збору розвідувальної інформації, забезпечення проведення притягнення до відповідальності злочинців, ефективного управління та підготовки персоналу, а також компетентного здійснення кримінального аналізу на усіх етапах та напрямах зазначеної діяльності.

Кримінальний аналіз як інструмент, на шляху технологічних інновацій, є надзвичайно важливим у контексті глибокого впливу на політику, стратегію та практику поліцейської діяльності. Базовими спроможностями кримінального аналізу стало ефективне та результативне виявлення моделей, серій і тенденцій злочинів. Технологічний розвиток систем геолокації та мапування, підвищення прозорості поліцейської діяльності в громадах по забезпеченню громадського порядку та протидії злочинності, дозволили краще зрозуміти проблеми, що виникають у різних громадах, правоохоронні органи змогли розробляти більш комплексні заходи реагування, отримали змогу краще комунікувати з іншими установами, соціальними групами та громадянами.

Кримінальний аналіз в унісон з технологічним розвитком та цифровізацією суспільних відносин забезпечує ключові завдання – встановлення та затримання злочинців, зокрема квартирних злодіїв, викрадачів автомобілів, грабіжників, наркоторговців, членів організованих злочинних угруповань. Оволодіння статистичними методами та сучасними інструментами аналізу даних забезпечило професійний рівень роботи з великими даними, краще розуміння можливостей аналітичних про-

дуктів, розроблення кращої політики та стратегії, які виходять за рамки традиційних процесів або шаблонного мислення.

> *Трендовою особливістю кримінального аналізу стала проактивна діяльність, упровадження превентивних заходів у діяльності органів правопорядку.*

Новітня історія розглядає низку моделей правоохоронної діяльності, що акцентують увагу на різних функціональних складових: адміністративних, оперативно-розшукових, процесуальних; включають аспекти пошуку, збору інформації та обміну нею, а також аналітичної підтримки з метою ефективного управління та реагування на злочинність і порушення громадського порядку. Кримінальний аналіз в силу своєї інституційної належності до системи правоохоронної діяльності, займає відповідне функціональне місце щодо підтримки та упровадження кожної із відомих нових форм та моделей. Дослідники та правоохоронна література зазвичай методологію правоохоронної діяльності розкривають на основі п'яти моделей поліцейської діяльності [1], хоча насправді їх значно більше [2] (рис. 5.1), бо як характеризуються різними періодами активності, регіональними ініціативами та географічними особливостями.

Соціально-орієнтована поліцейська діяльність	Community Policing
Проблемно-орієнтована поліцейська діяльність	Problem-Oriented Policing (POP)
Комп'ютерна статистична модель поліцейської діяльності	Computer Statistics Model (CompStat)
Поліцейська діяльність, керована даними	Data-driven Policing
Прогностична поліцейська діяльність	Predictive Policing
Поліцейська діяльність на основі теорії розбитих вікон	Broken Windows Policing
Поліцейська діяльність, керована аналітичною розвідкою	Intelligence-led Policing (ILP)

Рисунок 5.1. Моделі правоохоронної діяльності

Кожна з цих моделей має різні стратегічні цілі, сильні та слабкі сторони та може доповнювати інші, коли вони використовуються одночасно. Наприклад, ILP все частіше використовується для посилення соціально-орієнтованої поліцейської діяльності, забезпечуючи конкретні процеси, процедури комунікації та структури управління зі збору, аналізу й розповсюдження даних та інформації. У межах традиційної поліцейської діяльності ILP застосовується тільки в системі протидії організованій злочинності.

Але потрібно зазначити, що ILP є якраз найінтелектуальнішою розвиненою моделлю, що вимагає відповідного рівня сприйняття і забезпечення всіма елементами правоохоронної системи.

СОЦІАЛЬНО-ОРІЄНТОВАНА ПОЛІЦЕЙСЬКА ДІЯЛЬНІСТЬ

Community Policing

Соціально-орієнтована поліцейська діяльність спрямована на зміцнення довіри й посилення комунікацій між правоохоронним органом та громадськістю. Ключовою метою community policing є відновлення репутації правоохоронних органів та підвищення довіри населення, «легітимізація» їхньої діяльності, вироблення нових стандартів поведінки та етики, передача процесу визначення пріоритетів у правоохоронній діяльності під контроль громади.

Соціально-орієнтована поліцейська діяльність є однією з найбільш поширених поліцейських стратегій за останні тридцять років [2; 3]. За даними Мастрокскі [2; 4], на певному етапі її запровадили майже 100% великих поліцейських управлінь у США. Community policing програми включають створення громадських форумів із залученням представників різних громадських груп та інститутів, де обговорюються й розглядаються питання безпеки, включаючи правопорушення та окремі злочини в регіоні. Взаємодія поліції з громадою робить акцент на зменшенні страху перед злочинністю та сприянні загальній безпеці шляхом покращення взаємодії з громадою. Крім того, це стратегія, за допомогою якої поліцейські відділи прагнуть вирішити проблеми злочинності та громадського

порядку через державне та приватне партнерство з громадами, яким вони служать [2; 5; 6]. Основні теми взаємодії поліції з громадою включають підвищення прозорості для громади, підтримання збалансованих відносин, які заохочують внесок та участь громади, а також сприяння повсякденному спілкуванню з нею.

Взаємодія поліції з громадою – це не просто стратегія, на думку експерта з питань Community policing Гері Корднера [2; 7], вона має три виміри: філософський, програмний та стратегічний. «Філософський» стосується головних цінностей департаменту і того, що, на думку його членів, він повинен робити. «Програмний» стосується того, як саме будуть досягнуті філософські цілі. «Стратегічний» – це щоденна діяльність відділу і те, як вона організована. Разом ці компоненти допомагають створити унікальну стратегію взаємодії поліції з громадою, залежно від основних цінностей, цілей та оперативної структури відомства.

> *Community policing, як правило, більше зосереджена на питаннях якості життя, ніж на серйозних проблемах зі злочинністю.*

Іншими словами, громаду більше турбує процесуальна справедливість – тобто, щоб поліція вчасно реагувала на їхні проблеми, визнавала їхні скарги, ставилася до них з повагою і справедливістю [2; 8; 9; 10]. Як наслідок, вимірювані результати включають час, витрачений на вирішення проблем, час, витрачений на роботу з громадськими групами та мешканцями, кількість проактивних проєктів, кількість контактів з громадою, кількість звернень за допомогою, а також сприйняття місцевим населенням безпеки та поліції [2; 5; 6; 11].

Існує безліч досліджень та емпіричних оцінок ефективності взаємодії поліції з громадою [2; 12]. Результати були неоднозначними, але загальний висновок полягає в тому, що його вплив на реальний рівень злочинності є мінімальним. У своєму огляді ефективності поліцейських практик Телеп і Вайсбурд дійшли висновку, що загалом «програми взаємодії поліції з громадою мають незначний вплив на рівень злочинності й більш суттєвий вплив на підвищення рівня задоволеності громадян і сприйняття ними законності» [2; 13].

COMMUNITY POLICING & CRIME ANALYSIS

Кримінальний аналіз є невід'ємною та необхідною складовою підтримки взаємодії поліції з громадою, надаючи критично важливу інформацію для кращого розуміння різних проблем і питань, що турбують громаду. З оперативної точки зору, залежно від рівня технологій, кримінальний аналіз надає статистичні дані щодо попиту на інформацію про злочинність і порушення громадського порядку.

Якість поліцейських послуг у громадах залежить від здатності ефективно збирати, порівнювати, аналізувати та поширювати відомості про стан криміногенної ситуації у адміністративно-територіальних одиницях. Розуміння загального стану якості поліцейської роботи та стану злочинності має обмежений характер. Попри те, що поліція оперує значним обсягом даних про стан справ, лише зусиллями аналітиків представляється можливим вивчення широкого спектру складових, сукупність яких формує дійсний стан криміногенної ситуації в кожній окремій громаді та країні в цілому. Аналітики підрозділів кримінального аналізу здатні систематично досліджувати значні обсяги даних, щоб розвинути комплексне уявлення про різні адміністративні, технологічні та операційні аспекти функцій поліцейського підрозділу щодо безпеки в громадах та протидії злочинності.

Кримінальний аналіз є засобом аналізу статистичних даних щодо злочинності та порушення громадського порядку, оскільки завдяки застосуванню аналітичного процесу представляється можливим виявляти закономірності та тенденції, напрями руху криміногенної ситуації. Аналітики виконують важливу роль у складанні профілів потенційних злочинців, потерпілих, що турбують мешканців громад, та поширених кримінальних патернів. Також аналітики ідентифікують та оцінюють загрози, з якими може зіштовхнутись орган поліції у майбутньому, залежно від зміни соціальної кон'юнктури. Аналітики підрозділів кримінального аналізу з різним рівнем вірогідності досліджують події минулого з метою підготовки прогнозів, які у підсумку відіграють ключову роль у підготовці не лише оперативних відповідей, а й політики та векторів розвитку поліції як в окремих громадах, так і у цілій країні.

Крім того, кримінальний аналіз може інтерпретувати дані на спеціальних географічних рівнях, таких як дільниці, групи, мікрорайони, сегменти вулиць або будь-яка інша визначена територія, яка потребує більшої уваги. Завдяки добре реалізованому кримінальному аналізу вдається оперувати даними географічного сегменту, що дозволяє співробітникам поліції мати проаналізовану

інформацію про ті частини громади (ділянки місцевості), які потребують посиленої уваги з боку поліції. Маючи доступ до інформації на «мікрорівнях», поліція може ефективніше реагувати на конкретні проблеми, що виникають у громаді, й отримати чітке уявлення про проблеми до того, як вони вийдуть з-під контролю.

Завдяки кримінальному аналізу поліція має ширший арсенал виявлення, ідентифікації, оцінки як поодиноких проблем, так і системних проблемних явищ у кожній окремій територіальній громаді. Поліція має змогу оперативно та предметно готувати відповіді цим проблемам опираючись на підготовку персональних індивідуальних унікальних рішень, і застосовувати напрацьований досвід відповідей кримінальним викликам, яким властиво повторюватися.

Аналітики, маючи досвід проведення нарад та брифінгів зі співробітниками різних служб та підрозділів поліції, ЗМІ, можуть брати участь у зустрічах із місцевою громадою та надавати допомогу в організації таких зустрічей. Також аналітики мають значний досвід інтерпретації та візуалізації даних криміногенного характеру, які вони можуть доводити до мешканців громади, пояснювати відповідні статистичні дані громаді у більш прозорий спосіб, а також демонструвати карти, які надають візуальне уявлення про проблеми злочинності та громадського порядку, що у підсумку сприятиме отриманню допомоги від громадян, які матимуть певний рівень розуміння стану справ, і, якщо буде можливо, сприятимуть поліції у стабілізації ситуації.

Поширення у доступній формі відомостей про специфіку роботи поліції сприяє зменшенню недовіри до поліції, яка пересічним громадянам видається закритою інституцією. Зустрічі дають членам громади можливість поставити запитання та висловити свої занепокоєння, почути про реакцію поліції на поточні проблеми, а також отримати додаткову інформацію, про яку поліція могла б і не здогадуватися.

ПРОБЛЕМНО-ОРІЄНТОВАНА ПОЛІЦЕЙСЬКА ДІЯЛЬНІСТЬ (ПОП)

Problem-Oriented Policing (POP)

У проблемно-орієнтованій поліцейській діяльності ідентифікація та аналіз «проблем» є головним напрямом роботи правоохоронного органу, а робота з конкретним злочином, справою, викликом або інцидентом. У цій моделі особлива увага приділяється загальним проблемам злочинності та питанням безпеки. Правоохоронний орган активно вибудовує превентивну стратегію з можливістю вирішення проблеми, а не простого реагування на шкідливі наслідки.

ПОП є концептуальним підходом, за допомогою якого можливо вирішити безліч проблем в межах правоохоронної діяльності, але від цих структур вимагається глибше занурення в першопричини загроз для громадської безпеки. Правоохоронні органи повинні відфільтровувати наявні дані та інформаційні джерела для ідентифікації проблем, їх аналізу й пошуку причин – до реагування на проблему як таку.

> *Проблемно-орієнтована поліцейська діяльність – це система виявлення, аналізу та вирішення проблем злочинності [2; 14; 15].*

Щоб краще зрозуміти зміст ПОП, важливо її охарактеризувати у порівнянні з Community policing та CompStat. Так ПОП часто переплітається з Community policing, але ці моделі не є тотожними. Community policing є більш широкою організаційною філософією, яка включає в себе принципи ПОП, але також передбачає розвиток зовнішніх партнерських відносин із зацікавленими сторонами в громаді. Крім того, Community policing передбачає організаційні зміни (наприклад, децентралізацію прийняття рішень, закріплення географічної підзвітності, навчання в масштабах всієї організації та атестацію персоналу), спрямовані на підтримку спільного вирішення проблем, партнерства з громадою та загальну проактивну націленість на боротьбу зі злочинністю та соціальними заворушеннями. За умови належного виконання, Community policing забезпечує сильну всеохоплюючу філософію, в межах якої ПОП може існувати й процвітати. Крім того, орган взаємодії поліції з громадою, який не дотримується принципів ПОП, навряд чи зможе суттєво вплинути на зниження рівня злочинності [2]. Частиною процесу ПОП є визначення партнерів, які можуть запропонувати допомогу у вирішенні конкретних проблем, як у випадку Community policing.

ПОП набув практичного значення з впровадженням моделі SARA (Scanning, Analysis, Response and Assessment – *сканування, аналіз, реагування та оцінка*), яка допомагає практикам впроваджувати процес вирішення проблем [2; 16]. Вайсбурд та його колеги [2; 17], досліджували ефективність про-

блемно-орієнтованих поліцейських заходів. Аналіз проблемно-орієнтованої поліцейської діяльності показав, що ця методика має скромний, але статистично значущий вплив на зниження рівня злочинності та порушення громадського порядку. Автори також зібрали більш численні, але менш ретельні дослідження до/після впровадження без групи порівняння; результати цих досліджень вказують на переважний позитивний вплив ПОП.

ПОП притаманна відповідна синергія із ILP, оскільки обидва підходи об'єднує пошук комплексних вирішень проблем з можливістю закріплення довготривалих результатів та вироблення стратегії мінімізації ризиків. Обидва підходи вимагають пошуку стратегічного рішення, але ILP більш чітко визначає роль правоохоронного органу, забезпечуючи підтримку довгострокового стратегічного менеджменту та притягнення правопорушників до відповідальності. Саме тоді поліція може бути достатньо проактивною та прогнозувати ризики, гарантуючи спокій і безпеку у довгостроковій перспективі.

POP & CRIME ANALYSIS

Кримінальний аналіз має важливе значення для успіху проблемно-орієнтованої поліцейської діяльності. Аналітики, які працюють за цією моделлю, надають різноманітну інформацію, що використовується протягом усього процесу SARA [2; 18; 19].

За використання моделі SARA (процес ідентифікації проблем, аналізу, реагування, оцінки та коригування відповіді) (рис. 5.2) формуються стійкі передумови для розкриття складних механізмів щодо проблем злочинності та упровадження конкретних заходів, які впливають на умови поширення таких проблем.



Рисунок 5.2. Модель SARA

Із запровадженням моделі SARA, ПОП набула ще більшого практичного значення, оскільки допомогла фахівцям-практикам упровадити у роботу під час вирішення складних проблем процес розв'язання їх на фаховому і методичному рівні з відповідним науковим рівнем.

Для того, щоб сформувати вичерпне та відповідне дійсності розуміння криміногенної ситуації, співробітникам поліції слід здійснити ***сканування*** середовища (**S**). Цей крок вимагає від співробітників поліції здійснити виявлення потенційних проблем та провести їх ранжування (пріоритизацію) на території діяльності окремого правоохоронного органу.

Правопорушення вчиняються у певних місцях та відносно конкретних людей, тому значним обсягом інформації про кримінальну активність володіють саме члени громади. Діяльність з пошуку проблем у значній мірі залежить від уміння налагоджувати контакти з місцевим населенням (членами громади). Отримання інформації від членів громади про злочини, криміногенні місця, про потенційних правопорушників та інші проблеми, які підвищують ризик злочинності, а також заходи на основі цієї інформації, у підсумку є суттєвими факторами впливу на зниження рівня злочинності.

Проведення сканування можна описати на кількох прикладах [20].

> *Поліцейський, взаємодіючи з населенням, перебуваючи на місцях, з'ясовує у мешканців інформацію, якою вони можуть володіти, про будь-які протиправні прояви (кримінальні чи адміністративні), що мали місце в минулому та спостерігалися цими мешканцями.*
>
> *Також співробітникам поліції доцільно надавати місцевим мешканцям номери телефонів, за якими вони можуть анонімно залишати відомості для поліції про обставини, які викликають занепокоєння, якщо вони не бажають спілкуватися з поліцією публічно.*
>
> *Співробітники поліції можуть запитувати про проблеми злочинності та ідеї щодо їх вирішення на регулярних (наприклад, щомісячних) зустрічах громад або міжвідомчих нарадах.*
>
> *Співробітники поліції можуть використовувати опитування громад, представників середніх та малих підприємств, інші категорії населення. На додаток до відповідей на традиційні запитання щодо загального задоволення станом криміногенної ситуації респондентів просять визначити конкретні проблеми злочинності.*

На другому етапі (**A**), застосування моделі SARA, проводиться ґрунтовний ***аналіз*** отриманих даних, наприклад,

> *аналіз часу доби, коли відбуваються інциденти, визначення тих, хто є правопорушниками, і чому вони віддають перевагу, до прикладу, парковій зоні для вчинення протиправних дій;*
>
> *аналіз дозволяє досліджувати конкретні зони парку, які найбільш сприятливі для протиправної діяльності; оцінюються характеристики такого простору для визначення чинників, які сприяють вчиненню правопорушень;*
>
> *аналіз тенденцій також проводиться з метою пошуку належної реакції з боку поліції;*
>
> *аналіз відомостей про проблеми дозволяє приймати рішення про те, як їм протидіяти – підготуватися до реагування.*

На третьому етапі – ***реагування*** (**R**) – співробітники поліції розробляють та впроваджують заходи, спрямовані на усунення причин та самих проблем. Здійснюючи діяльність щодо діагностики проблем та розробки рішень слід дотримуватись поетапного процесу. Цей процес акцентує увагу на розумінні проблем та їх причин, розробці та перевірці рішень, а також із врахуванням практичного досвіду працівників поліції.

У розгорнутому форматі процес діагностики проблем та розробки рішень складається з таких етапів:

- ✓ *ретельне дослідження ситуації;*
- ✓ *чітке формулювання проблеми;*
- ✓ *вибір конкретної проблеми для реагування (реакції);*
- ✓ *збір та обробка даних про проблему;*
- ✓ *аналіз причин виникнення проблеми;*
- ✓ *розробка плану вирішення проблеми;*
- ✓ *перевірка (тестування) плану вирішення проблеми;*
- ✓ *оцінка результату перевірки (тестування) способу вирішення проблеми;*
- ✓ *впровадження рішення у реалізацію;*
- ✓ *оцінка якості процесу реалізації рішення проблеми, а згодом – перехід до наступної проблеми [20].*

Останнім кроком застосування моделі SARA є аналітична ***оцінка*** (**A**), що включає оцінку реагування поліції та результатів, яких вдалось досягти.

> **Приклад**. *Відділ поліції може визначити, що злочинність, пов'язана з наркотичними речовинами зростає, що становить проблему, яка потребує вирішення (фаза сканування). Подальше вивчення природи злочинів, пов'язаних з наркотиками, може виявити проблемні ділянки місцевості та окремі часові періоди кримінальної активності (фаза аналізу). На основі цього аналізу поліція може вирішити спрямувати посилене патрулювання та правоохоронні заходи в конкретні райони, які вважаються проблемними в конкретний час, а також співпрацювати з громадськими організаціями для реалізації програм лікування від наркотичної залежності (фаза реагування). Через певний період часу відділ поліції може порівняти рівень злочинності, пов'язаної з наркотиками, в цілому на території обслуговування, а також у цільових областях, до та після впровадження відповіді (фаза оцінки).*

Можна з упевненістю сказати, що без реального аналізу злочинності ПОП не був би настільки поширеним і не мав би такого значного позитивного впливу на проблеми злочинності та громадської безпеки, як на сьогоднішній день [2; 21]. Корисність цієї моделі найкраще ілюструється безліччю проектів, які були реалізовані в межах ПОП, та численними посібниками, розробленими, дослідженими та написаними Центром ПОП за фінансової підтримки Міністерства юстиції США та поліції. На сьогоднішній день існує 92 посібники POP [2], в яких розглядаються деякі з найбільш поширених проблем злочинності, способи реагування та інструменти, які можуть бути використані й застосовані на місцях тими, хто стикається з подібними проблемами. Деякі з тем включають графіті, крадіжки з магазинів, шахрайство з рецептами, крадіжки з автомобілів на автостоянках, розгул молоді в громадських місцях, а також напади в барах та біля них. Кожен посібник містить розділ, що націлює на вирішення проблеми, включаючи інформацію та перспективи, які аналітик підрозділу кримінального аналізу може використати для ефективного розуміння та оцінки проблеми у своїй юрисдикції.

У межах моделі ПОП аналітики тісно співпрацюють з військовослужбовцями, яким доручено розслідувати певну проблему. Проблема, що розглядається, може бути короткостроковою; однак ПОП

зазвичай використовується для вирішення довготривалих проблем, які потребують стратегічного підходу. Таким чином, етап аналізу є критично важливим для процесу; його відсутність призведе до неправильного визначення проблеми. Крім того, перехід від сканування до реагування в межах моделі SARA без проведення належного аналізу та оцінки після впровадження є, по суті, марнуванням ресурсів у короткостроковій і довгостроковій перспективі. Особливо це стосується випадків, коли рішення про реагування зводиться до простого посилення патрулювання, яке не завжди є ефективним і може призвести до переміщення на схожі території чи цілі або до поновлення проблеми після перенаправлення ресурсів в інше місце. Нарешті, одним з найважливіших ключів до ефективного ПОП є те, що аналітики витрачають час на відвідування й спостереження за місцем виникнення проблеми, а також на аналіз даних, щоб переконатися, що контекст проблеми зафіксовано. Проблеми не можуть бути повністю проаналізовані, якщо не враховувати належний контекст. Саме тут ПОП може часто перетинатися з охороною громадського порядку, оскільки громадяни та власники бізнесу у визначеному районі можуть поділитися інформацією про історію та культуру, а також про справжній масштаб проблеми [2].

КОМП'ЮТЕРНА СТАТИСТИЧНА МОДЕЛЬ ПОЛІЦЕЙСЬКОЇ ДІЯЛЬНОСТІ

CompStat

У 1994 році комісар поліції Нью-Йорка Вільям Бреттон запровадив модель управління на основі даних під назвою CompStat, яка сприяла зниженню рівня злочинності та підвищенню якості життя в місті. [2; 22; 23; 24; 25]. Хоча залишаються суперечки щодо походження назви (наприклад, Комп'ютерна статистика (*Computer Statistics*), Порівняльна статистика (*Compare Statistics*)), модель CompStat – це процес управління в межах системи управління ефективністю, яка поєднує аналіз даних про злочинність і порушення громадського порядку, стратегічне вирішення проблем і чітку структуру підзвітності [2; 25; 26]. CompStat – це система управління на основі розробленої моделі, у якій менш тяжкі злочини розглядаються елементом зниження кількості більш тяжких злочинів. Таким чином, на підставі аналізу статистики вчинених злочинів окремі регіональні керівники правоохоронних органів є відповідальними за впровадження на місцевому рівні розроблених завчасно заходів.

Модель підкреслює залежність від точного і своєчасного аналізу та виявлення патернів злочинів й проблем, для вирішення яких застосовуються спеціальні заходи реагування шляхом швидкого розгортання персоналу й ресурсів.

> *Система звітності CompStat має ключове значення для забезпечення того, щоб аналіз був врахований, а заходи реагування реалізовані належним чином, а також для оцінки їх ефективності [22; 27].*

На відміну від реактивної, традиційної моделі правоохоронної діяльності, яка сприяє «управлінню кризою», CompStat є інновацією, яка надає правоохоронним органам проактивні засоби, що дозволяють їм діяти на основі ретельно розробленого аналізу та звітувати про послідовні показники діяльності, які пов'язані з місією відомства. Правоохоронні органи, які долають обмеження традиційної правоохоронної моделі, стають більш цілеспрямованими, менш схильними до ризику й більш прозорими [2]. Крім того, модель CompStat надає відомствам можливість реструктурувати свою систему управління для покращення розподілу ресурсів, партнерства з іншими державними установами та надання послуг громадянам. Деякі відомства вважають застосування CompStat корисним і в інших сферах, таких як антикорупційні підрозділи поліції, внутрішніх розслідувань та боротьби з тероризмом [2; 26].

Завдяки своєму успіху в Нью-Йорку CompStat швидко поширився в американських правоохоронних органах, перетворившись на загальноприйняту модель управління. У 1999-2000 роках понад третина відомств з чисельністю 100 і більше співробітників повідомили про впровадження програми, подібної до CompStat [2; 27].

CompStat часто плутають з моделлю ILP. CompStat концентрується, в основному, на вуличних та серійних злочинах із забезпеченням короткострокової підзвітності в процесі вирішення нових кримінальних викликів; ILP включає довгостроковий стратегічний компонент, який може бути застосований і під час операцій з протидії транснаціональній організованій злочинності. CompStat фокусується на злочинності, а ILP – на ідентифікації загроз.

COMPSTAT & CRIME ANALYSIS

Кримінальний аналіз є надзвичайно важливим для моделі CompStat, оскільки вона значною мірою залежить від точних і своєчасних статистичних даних та інформації, які потребують опрацювання та правильної інтерпретації досвідченими аналітиками.

Хоча процес у межах моделі CompStat залежить від конкретної правоохоронної структури, часто більшу частину свого часу аналітики витрачають на підготовку до наступної наради звітів і карт поширення злочинів та правопорушень для визначення «гарячих точок» (Hot Spot).

Хоча процес CompStat характеризується значною варіативністю в різних відомствах, аналітики завжди виконують ключову роль, оскільки значна частина їхнього часу витрачається на підготовку звітів, мап і нарад. Хоча така зосередженість на статистиці може перешкоджати проактивному кримінальному аналізу, CompStat допомагає відділкам поліції бути поінформованими щодо найактуальніших проблем злочинності та порушень громадського порядку, які можна оцінити практично на будь-якому географічному вимірі [2]. Модель CompStat також заохочує поліцейський персонал, у тому числі керівників, до розширення взаємодії та спілкування з аналітиками підрозділів кримінального аналізу для поглиблення знань та розуміння поточних проблем у своїх підрозділах. Водночас це зорієнтовує керівників та інший персонал на виважений запит необхідної інформації та аналітичних звітів та знаходження шляхів вирішення нових і довгострокових проблем.

Наради, які є необхідним елементом цієї моделі, проводять з достатньо різною періодичністю (місяць, квартал) [29; с. 270]. Водночас фахівці зазначають, що часто аналітикам надається відносно мало часу для проведення ґрунтовних досліджень [29; 30], що є основним недоліком CompStat. Однак вирішення цієї проблеми розглядають у розширенні партнерства між поліцейськими відділами та професійними дослідниками, що може бути надзвичайно цінним.

> *Вкрай важливим інструментом розширення спроможностей стратегічного кримінального аналізу є налагодження співпраці з академічними та дослідницькими програмами кримінологічного та соціологічного спрямування, які можуть використовувати додаткові позабюджетні (грантові) ресурси та власний персонал. IACA [2]*

ПОЛІЦЕЙСЬКА ДІЯЛЬНІСТЬ, КЕРОВАНА ДАНИМИ

Data-driven Policing

Усі моделі поліцейської діяльності потребують використання певного сховища даних, яке у подальшому використовується у процесі реалізації тактичних та стратегічних цілей, аналізу та планування розподілу ресурсів, планування роботи поліцейських патрулів тощо. Серед варіантів підходів, заснованих на даних, найбільше привертають увагу – підходи, керовані даними, щодо злочинності та безпеки дорожнього руху (*Data-Driven Approaches to Crime and Traffic Safety – DDACTS*). DDACTS – це операційна модель, за якою поліцейська діяльність орієнтується на фактичні події, що мають місце в громадах. Такий підхід надає правоохоронним органам альтернативну модель для розгляду в умовах зростаючого попиту на реагування щодо проблеми громади, незважаючи на обмежені ресурси [2; 31].

> *DDACTS інтегрує дані про аварії, злочинність, виклики служб та правоохоронні органи з прив'язкою до місцевості для створення ефективних та дієвих методів розгортання ресурсів правоохоронних органів.... Спираючись на стримуючу цінність добре помітного контролю за дорожнім рухом і знання того, що злочини часто пов'язані з автотранспортом, метою DDACTS є зменшення аварійності, злочинності та соціальної шкоди в громадах по всій країні. IACA [2]*

DDACTS складається з чотирьох основних підходів: стратегічного, тактичного, проблемно-орієнтованого та орієнтованого на правопорушника. Стратегічний підхід спрямований на надання обґрунтованих прогнозів щодо «гарячих точок» злочинності та дорожньо-транспортних пригод. Тактичний підхід спрямований на виявлення нових «гарячих точок» і спирається на методи аналізу рядів та/або порогових значень. Проблемно-орієнтований підхід зосереджений на довгострокових закономірностях і визначає окремі проблеми зі злочинністю, порушеннями громадського порядку та аварійністю в межах цільових районів. Нарешті, підхід, орієнтований на правопорушників, намагається використовувати інформацію про відомих злочинців, кримінальні організації та їх маршрути переміщення з метою збору оперативних даних, обмеження активності правопорушників і проведення арештів за порушення правил обігу наркотиків, зброї та викрадення майна.

DDACTS зазначає про необхідність коректної роботи з даними та вказує на конкретні проблеми, що мають місце на практиці [2]:

- *обмеженість даних за попередні періоди, що суттєво впливає на можливості встановлення основних тенденцій та закономірностей;*
- *автоматизовані системи управління мають обмежені можливості щодо експорту даних;*
- *помилки під час кодування за категоріями злочинів, аварій або викликів швидкої допомоги;*
- *велика кількість недійсних або неправильних адрес;*
- *для даних про аварії не передбачено введення факторів щодо причинно-наслідкових зв'язків;*
- *своєчасність введення даних;*
- *дублювання записів.*

DDACTS & CRIME ANALYSIS

DDACTS є спеціалізованою моделлю, а тому вимагає достатньої обізнаності проблемами безпеки дорожнього руху та злочинності в аналітика. Водночас, DDACTS не є широко впровадженою моделлю, порівняно з іншими, і є більш сприйнятливою для альтернативних і нетрадиційних підходів [2].

Аналітики, які працюють з DDACTS, витрачають багато часу на аналіз даних, пов'язаних з дорожнім рухом (наприклад, гарячі точки ДТП, порушення правил дорожнього руху в стані алкогольного сп'яніння, гарячі точки викрадення автомобілів, інциденти зіткнень з травмуванням, випадки необережного водіння), які накладаються на інформацію про злочинність для виявлення нових закономірностей [2; 32]. Наприклад, аналітик може виявити, що в районі з високим рівнем вуличних пограбувань також спостерігається високий рівень дорожньо-транспортних пригод. Такий аналіз може допомогти розподілити обмежені ресурси підрозділу поліції, а також підвищити обізнаність громадськості про потенційні небезпеки на дорогах і проблеми зі злочинністю [2].

ПРОГНОСТИЧНА ПОЛІЦЕЙСЬКА ДІЯЛЬНІСТЬ

Predictive Policing

В основі Predictive Policing запозичення підходів POP та Data-driven моделей [2]. Ця стратегія, яка часто використовується як синонім терміну «crime forecasting», так само зосереджена на використанні передової аналітики для «інформування про перспективні зусилля щодо запобігання злочинності» [33, с. 1].

> *Прогностична поліцейська діяльність включає в себе різноманітні статистичні методи в поєднанні з програмним забезпеченням та на основі інформації про громаду і попередні інциденти, зорієнтована на передбачення найбільш ймовірного виникнення злочинів чи порушень громадського порядку [2; 32; 34].*

Однак важливо зазначити, що прогностична поліцейська діяльність не є програмним пакетом, який можна купити в магазині [35]. Predictive policing покладається на точні та надійні статистичні дані. Тому, застосовуючи модель прогностичної поліцейської діяльності, надзвичайно важливо забезпечити чітку впевненість поліцейського персоналу щодо систем даних, які ними використовуються. Це можна встановити за допомогою [2]:

- ✓ *залучення добре підготовлених аналітиків, які мають повне бачення щодо сильних і слабких сторін даних, що використовуються;*
- ✓ *проведення систематичних перевірок даних для забезпечення їх точності, узгодженості та надійності;*
- ✓ *перегляд результатів прогнозування для впевненості щодо їх обґрунтованості та логічності – іншими словами, впевненість в тому, що для зроблених прогнозів, існує підтверджуюча інформація, включаючи місця, що приваблюють злочинність, звіти про осіб, щодо яких є інтерес у певній місцевості, нещодавні звіти про опитування на місцях, а також нещодавні місця вчинення злочинів та їх описи [32].*

Predictive policing не тільки дає змогу встановити місце можливого вчинення злочину в найближчому майбутньому, але й допомагає виявити потенційних правопорушників та жертв злочинів [2; 32]. У той час як такі методи, як виявлення «гарячих точок» і моделювання ризикових зон, можуть допомогти виявити потенційні майбутні правопорушення, потенційних злочинців можна ідентифікувати за допомогою вивчення розвідувальної інформації щодо організованої злочинності або використання методів регресії. Прогностичні аспекти щодо злочинців передбачають отримання висновків зі звітів кримінальної розвідки та використання інструментів географічного профілювання. Прогнозування віктимізації може складатися з деталізації кримінальних історій відомих

рецидивістів та використання передових методів аналізу даних [2]. Водночас фахівці вказують на певні проблеми, пов'язані з прогностичною поліцейською діяльністю – потенційно можливе порушення питань конфіденційності та громадянських свобод через обмін інформацією. Прихильники Predictive Policing наголошують на важливості вирішення проблем конфіденційності шляхом проведення всебічного аналізу політики, її вдосконалення та посилення підзвітності [2; 34].

PREDICTIVE POLICING & CRIME ANALYSIS

Кримінальний аналіз є надзвичайно важливим щодо упровадження та розвитку парадигми прогностичної поліцейської діяльності. Існує безліч програмних пакетів (як комерційних, так і безкоштовних), які надають інструменти, що полегшують отримання прогностичної поліцейської інформації. Однак ключем до отримання дієвих результатів є достовірні та надійні дані, перекладені та інтерпретовані аналітиками, які повинні повністю усвідомлювати сильні та слабкі сторони даних, що використовуються ними, щоб забезпечити надійність прогнозів злочинності та порушень громадського порядку для оперативних і тактичних цілей [2]. Крім того, аналітики повинні розглянути можливість залучення нетрадиційних джерел даних (наприклад, дані про комунальні послуги, транспортні дані), щоб охопити елементи, які зазвичай вважаються «нестандартними», але які все одно можуть виявитися корисними [34].

Основним завданням аналітиків підрозділів кримінального аналізу є надання інформації, яка допоможе розгортанню поліцейського підрозділу в необхідних місцях і в необхідний час для максимально ефективної та результативної протидії злочинності та порушеннями громадського порядку [2]. Для цього вони повинні мати доступ до GIS, баз даних SQL, інструментів передачі даних і статистичних пакетів, а також знати різні типи моделей прогнозування (одновимірні, багатовимірні тощо) [35].

Прогностична поліцейська діяльність не обмежується будь-якими попередньо встановленими інструментами. Аналітики, які використовують ці програми й пакети, мають можливість застосовувати будь-яку комбінацію опцій, включаючи аналіз близьких до повторення подій, аналіз гарячих точок, моделювання місцевості з підвищеним ризиком, географічне профілювання й методи інтелектуального аналізу даних, щоб найкращим чином вирішити наявні проблеми. Наприклад, перед аналітиками часто стоїть завдання скласти прогноз злочинності на наступний рік. Це завдання допомагає полегшити потенційні зміни в кадровому забезпеченні поліцейських відділів через незмінну проблему: обмеженість ресурсів [2].

Одне зі старих емпіричних правил прогнозування злочинності полягає в тому, що для того, щоб отримати прогноз злочинності на один місяць, необхідно використовувати дані щонайменше за три роки. Можна сперечатися про те, чи є це правильним, але цей приклад демонструє, що прогнозування злочинності не є точною наукою. Ця модель постійно вдосконалюється на основі нових математичних алгоритмів, розроблених для підтримки наявних інструментів, й існує безліч факторів і джерел, які можна логічно враховувати під час прогнозування злочинності та порушень громадського порядку [2]. Як мінімум, прогностична поліцейська діяльність повинна бути інтегрована з іншими тактичними заходами, а поліцейські відомства повинні остерігатися типових помилок, які можуть виникнути [32].

ПОЛІЦЕЙСЬКА ДІЯЛЬНІСТЬ НА ОСНОВІ ТЕОРІЇ РОЗБИТИХ ВІКОН

Broken Windows Policing

Модель розбитих вікон була представлена в 1982 році з публікацією короткої статті в журналі «The Atlantic», авторами якої були Джеймс К. Вілсон і Джордж Л. Келлінг. Завдяки своїй простоті та політичній привабливості метод розбитих вікон поширився по всій території США та в усьому світі, багато в чому вплинувши на поліцейську практику [26].

На противагу моделі ПОП, за якою конкретні рішення для різноманітних проблем, що виникають у поліції, з'являються в результаті ретельного і детального аналізу причин, зацікавлених сторін й особливостей місцевості, модель «розбитих вікон» пропонує одне загальне рішення для кожної проблеми: примусове виконання відносно незначних порушень, пов'язаних з неввічливістю, відсутністю порядку й пошкодженням майна. Цей підхід базується на двох принципах. По-перше, дрібні правопорушення можуть накопичуватися й ставати шкідливими для життя громади. Наприклад, викинути один пакунок сміття – не таке вже й страшне правопорушення, але якщо так робитимуть усі, то район перетвориться на віртуальне звалище. По-друге, дрібні правопорушення призводять до більших і заохочують до них. Наприклад, занедбані та забиті дошками будинки часто стають

місцем для наркоторгівлі та можуть породжувати інші, більш серйозні злочини. Разом ці висновки призвели до того, що деякі міста почали приділяти набагато більше уваги боротьбі з дрібними правопорушеннями та покращенню безпосереднього оточення [2].

Застосовуючи модель розбитих вікон, окремі відомства повинні вирішити, які незначні правопорушення матимуть пріоритет над іншими. Наприклад, керівники нью-йоркського метрополітену дізналися, що молоді люди, які перестрибують турнікети, щоб проїхати безкоштовно, часто і є грабіжниками в системі метрополітену. Контроль над дрібними злочинами (наприклад, безквитковий проїзд) допоміг зменшити кількість реальних пограбування [2]. З іншого боку, керівники метрополітену також дізналися, що ті, хто малює графіті, зазвичай не вчиняють більш серйозних злочинів під час поїздки, бо, не зважаючи на те, що зусилля по боротьбі з графіті були дуже ефективними, вони не знизили рівень пограбувань [36].

BROKEN WINDOWS POLICING & CRIME ANALYSIS

Кримінальний аналіз на принципах «Broken Windows» зосереджує основну увагу на інцидентах, пов'язаних із порушенням громадського порядку, що може призвести до певної неправомірної поведінки з наслідками вчинення більш значного злочину. Порушення громадського порядку у цьому контексті означає такі інциденти, як графіті, вандалізм, хуліганські проступки та зберігання наркотиків [2]. Аналітики також можуть досліджувати громадські та комерційні заклади, які можуть регулярно ставати гарячими точками інцидентів, пов'язаних з порушенням громадського порядку. За сприяння керівництва поліції аналітики можуть співпрацювати з цими закладами для підвищення безпеки відвідувачів та мешканців громади всередині та навколо закладу [19]. Інші зусилля цього ж напряму включають більш тісну співпрацю з громадою з питань порушення громадського порядку та отримання більшої підтримки для допомоги в прибиранні та утриманні громадської та приватної власності в районі. Оскільки порушення громадського порядку часто вчиняються підлітками та молодими людьми, аналітики можуть доповнити дослідження з питань порушення громадського порядку демографічною статистикою для моніторингу взаємозв'язків між ними. Ця інформація може бути інтегрована та передана соціальним службам, громадським організаціям, які можуть надавати послуги та допомагатимуть у зменшенні подальших порушень громадського порядку, а також злочинів, що вчиняються молоддю [2].

Іншим прикладом застосування кримінального аналізу в системі поліцейської діяльності на принципах «Broken Windows» є дослідження злочинності на пустирищах та навколо них. Хоча ці місця та споруди перебувають у приватній власності, вони іноді занедбані, піддаються руйнуванню та наркоторгівлі просто неба, що негативно впливає на навколишню громаду. Детальний аналіз порожніх ділянок може бути доведений до керівництва поліції та, зрештою, винесений у центр уваги політиків на рівні міста або територіальної громади, де будуть розроблені комплексні заходи для запобігання ескалації злочинної діяльності та її поширенню на прилеглі території [2].

> *Загальним фактором для більшості вищезазначених моделей, який нерідко характеризує слабку сторону сучасних правоохоронних органів, є їх спрямованість на локальні регіони і загрози. Значні зміни глобального масштабу змінили кримінальне середовище, разом з тим, названі методології, не наділені необхідними інструментами і характеристиками протидії більш системним кримінальним загрозам. І тільки ILP є єдиним методом, що позиціонується у цьому випадку як ефективна протидія.*

ПРАВООХОРОННА ДІЯЛЬНІСТЬ, КЕРОВАНА АНАЛІТИЧНОЮ РОЗВІДКОЮ

Intelligence-led Policing (ILP)

Правоохоронна діяльність, керована аналітичною розвідкою, є найбільш поширеною з нинішніх змін у філософії протидії злочинності та правоохоронного менеджменту. У поліцейський лексикон цей термін уперше увійшов у Великій Британії в 90-х роках як *Intelligence-led Policing (ILP)*. Виник він також у Великій Британії з того, що раніше називалося Кентською моделлю [37]. Рушійні сили для цього переходу поліцейської діяльності до нової стратегії були як зовнішніми, так і внутрішніми. У Великій Британії в кінці 1980-х і початку 1990-х років на тлі зростаючої тенденції рівня злочинності сформувався суспільний запит і зростаючий заклик до поліції бути більш ефективною й економічною. Зовнішні фактори включали нездатність традиційної, реактивної моделі поліцейської діяльності справлятися зі швидкими глобалізаційни-

ми змінами, які розширили можливості транснаціональної організованої злочинності й усунули фізичні й технологічні бар'єри у сфері поліцейської діяльності.

Пошукові нової стратегії допоміг звіт Комісії з аудиту 1993 (Ревізійна комісія – незалежний орган, відповідальний за економне та ефективне використання державних коштів) щодо ефективності діяльності поліції, в якому було сформульовано три основних принципи ефективної боротьби зі злочинністю [38]: *існуюча система по суті і організації позбавлена інтеграції та ефективності; поліція не в змозі найкращим чином використовувати ресурси; а також більш ефективним буде зосередження уваги на боротьбі зі злочинцями (криміналітетом), ніж на злочинах (окремих діяннях).*

Звичайно ж, перше не виключає друге, мова йде, в першу чергу, про пріоритети. Таке початкове тлумачення є дещо обмеженим і в наступному, враховуючи досвід впровадження та функціонування ILP, більш ґрунтовно визначено мету та завдання сучасної моделі.

ILP дозволяє застосувати перспективний та проактивний підхід в управлінні поліцією. Її успішне застосування протягом останніх років у низці країн світу щодо протидії тяжкій злочинності та транснаціональним загрозам, стимулювало подальший розвиток концепції ILP від моделі, призначеної, головним чином, для протидії організованій злочинності, до більш загальної стратегічної бізнес-моделі з вирішенням широкого спектру проблем поліцейської діяльності на місцевому, регіональному та національному рівнях. Ця динаміка безпосередньо пов'язана з пошуком методів правоохоронної діяльності, які б дозволили поліції більш ефективно впливати на злочинність, поширення злочинності та її соціальні наслідки, в умовах обмежених ресурсів та вимоги щодо підвищення відповідальності.

Останніми роками потреба в поліцейському реагуванні та послугах перевищила наявні ресурси поліції, що зумовило необхідність визначення пріоритету та більш ефективного використання ресурсів правоохоронних органів. Водночас зросли політичні та суспільні очікування щодо підзвітності. ILP була представлена як варіант вирішення цієї проблеми, оскільки вона запропонувала громадськості обґрунтування та інструменти для аналізу й оцінки загроз, забезпечуючи більш документально підтверджені, прозорі та підзвітні процедури прийняття рішень щодо використання наявних ресурсів там, де вони найбільше потрібні.

> *«Не слід ставити під сумнів необхідність запровадження поліцейської діяльності, керованої аналітичною розвідкою (ILP). В умовах обмеженості бюджетів та ресурсів кожна відповідальна особа та організація повинні визначити пріоритети для вирішення основних проблем. З метою сприяння визначенню пріоритетів, рішення мають прийматися на основі фактів та аналітики, основою яких є інформація. ILP сприятиме оптимізації розподілу ресурсів і концентрації зусиль у більш структурований спосіб. Таким чином буде легше впоратися з дедалі більшою витонченістю та пристосовуваністю злочинців, які діють проти закону та порядку»,*
>
> *– Європейська служба зовнішніх зв'язків (EEAS) [1].*

Той факт, що екстремісти, пов'язані з нещодавніми терористичними інцидентами, включаючи терористів-одинаків, залишалися поза увагою правоохоронних органів, зумовив необхідність вироблення превентивного підходу та підкреслив необхідність всебічного обміну та централізованого аналізу відповідних даних та інформації. Усвідомлення того, що терористичні атаки та раннє виявлення інших серйозних інцидентів не можуть бути вирішені шляхом реагування, поставило ILP у центр уваги на міжнародній правоохоронній арені. Це стало очевидним після терактів 11 вересня, що відображено у висновках Комісія США 9/11 [1], яка дійшла висновку, щодо вчинення нападів відповідні органи на різних рівнях мали у своєму розпорядженні різноманітну інформацію, але через нездатність органів обмінюватися оперативними даними, їх не вдалося скоординувати для отримання загальної картини.

> *Ця модель набула значного поширення, особливо після нападу на Всесвітній торговий центр 11 вересня 2001 року, коли стала очевидною потреба в поліпшенні розвідувальних операцій, включаючи навчання, обмін інформацією та більш тісну співпрацю між відомствами на місцевому, державному та федеральному рівнях. IACA [2]*

Зазначене дало поштовх до впровадження нової моделі, однак правоохоронна діяльність, керована аналітичною розвідкою, *є концепцією, яка розвивається*. Незважаючи на те, що початкові спроби визначення ILP вказували на тактичний інструмент для локальної правоохоронної діяльності та для орієнтації на мережі організованої злочинності, сучасний підхід до сприйняття *Intelligence-led*

Policing вказує на модель процесу з організаційною інфраструктурою для підтримки того, як слід здійснювати правоохоронну роботу в цілому. Це більш широке уявлення про правоохоронну діяльність, керовану аналітичною розвідкою, все частіше пов'язується з ідеєю виявлення та аналізу проблеми або сприймається як основа для подолання кризових ситуацій.

> *Правоохоронна діяльність, керована аналітичною розвідкою, покликана кинути виклик домінуючій парадигмі реактивної поліцейської діяльності.*
>
> *Правоохоронна діяльність, керована аналітичною розвідкою, стала управлінською моделлю для рішень щодо обґрунтованого розподілу ресурсів, із урахуванням напрямів та сфер активності серійних злочинців, організованих злочинних угруповань та кримінального середовища. Іншими словами, «гарячі люди», «гарячі групи» та «гарячі місця».*
>
> *Це також філософія, яка робить більший акцент на обміні інформацією та спільних стратегічних рішеннях щодо проблем злочинності.*

ILP & CRIME ANALYSIS

Кримінальний аналіз відіграє життєво важливу роль в ILP, оскільки він допомагає передавати критично важливу інформацію для осіб, які приймають рішення, щоб зосередити їхні обмежені та цінні ресурси. Аналітики в середовищі ILP працюють з різноманітними джерелами даних і повинні вміти швидко і систематично синтезувати їх в дієву інформацію для своїх підрозділів.

> *У контексті ILP пошук інформації є першим проявом аналітичної розвідки, націлюючи на ініціативні та креативні алгоритми у роботі аналітиків підрозділів кримінального аналізу, а також розвідувальний сенс отримання достатніх за обсягом й достовірністю даних та необхідної за змістом інформації.*

Водночас на додаток до належної підготовки щодо доступу та отримання інформації з різних джерел даних, аналітики повинні забезпечити дотримання відповідних правил розповсюдження інформації.

> *Одним з найважливіших операційних аспектів для аналітиків, які працюють в середовищі ILP, є те, що їм дозволяється – і заохочується – бути проактивними, а не реактивними.*

Реактивність у роботі аналітиків підрозділів кримінального аналізу не є недоліком, бо завжди мають місце завдання такого характеру. Але одним з ключових аспектів ILP саме у сенсі аналітичної розвідки і є випередження кривої зростання злочинності, збереження здатності до стримування злочинної діяльності й недопущення її потрапляння в зону високого ризику та надзвичайної загрози. У новому «суспільстві ризику» поліція розглядається як джерело даних з управління ризиками для низки зовнішніх установ [1].

> *Виявлення та управління ризиками є невід'ємною частиною сучасної поліцейської діяльності. Належний підхід ILP до збору й аналізу даних та інформації дозволяє ідентифікувати й оцінювати ризики, зокрема в частині основних подій, географічних регіонів, видів злочинів, соціальної шкоди, небезпечних злочинців та кримінальних мереж.*

ILP модель виходить з того, що кримінальне середовище має постійну характерну складову в операційному середовищі правоохоронної роботи. Незважаючи на динамічність і плинність, постійну зміну за формою, складом та розміром, залишається реальністю те, що завжди буде існувати кримінальна обстановка, яку необхідно буде зрозуміти з метою здійснення ефективної операційної роботи.

Виходячи з розвідувальної аналітичної сутності, ILP модель передбачає можливість інтерпретації кримінального середовища на підставі інформації з внутрішніх та зовнішніх джерел. Водночас інтерпретація й передбачає професійну інтелектуальну роботу аналітика. На наступному етапі отримана інформація про кримінальне середовище (явище) передається у формі аналітичних матеріалів особам, які приймають рішення про вплив на це кримінальне середовище. Цей етап передбачає відповідне управлінське мислення осіб, що приймають рішення на підставі знань про стратегії протидії злочинності, її скорочення або запобігання, а також здійснення впливу на злочинне середовище.

> *У контексті ILP ключовим оперативним аспектом також є те, що аналітики підрозділів кримінального аналізу НПУ розвивають і підтримують позитивні відносини з колегами в середовищі ILP, забезпечуючи відповідний рівень обміну даними та інформацією.*

Для того, щоб інформація безперервно обмінювалася між суб'єктами кримінальної юстиції, необхідно побудувати певний рівень довіри; аналітики можуть і повинні бути основою для регіональної комунікації.

> *Аналітики підрозділів кримінального аналізу НПУ набувають особливої відповідальності у процесі безпосереднього долучення до забезпечення суспільної безпеки, оскільки за цих обставин їхня функція з суто допоміжної перетворюється на ключовий компонент етапу планування стратегій та прийняття рішень.*

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *OSCE Guidebook Intelligence-Led Policing* (2017). TNTD/SPMU Publication. Series Vol. 13. Vienna.
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, KS: Author.
3. Skogan, W G. (2006). The promise of community policing. In D. Weisburd & A. A. Braga (Eds.), *Police innovation: Contrasting perspectives* (pp. 27-43). New York, NY: Cambridge University Press.
4. Mastrofski, S.D., Willis, J.J., & Kochel, T.R. (2007). The challenges of implementing community policing in the United States. *Policing*: *A Journal of Practice and Policy*, (1), 223-234.
5. Tonry, M. &r Morris, N. (Eds.) (1993). Modern policing. *Crime and Justice*, (15). Chicago, IL: University of Chicago Press.
6. Greene, J. (2000). Community policing in America: Changing the nature, structure, and function of the police. In *Policies, Processes, and Decisions of the Criminal Justice System*, Volume 3 (299-370). Washington, DC: U.S. Department of Justice, Office of Justice Programs.
7. Cordner, G. (1997). Elements of community policing. In L.K. Gaines & G.W Cordner (Eds.), *Policing perspectives: An anthology* (pp. 137-149). Los Angeles: Roxbury
8. Tyler, T. (1988). What is procedural justice? Criteria used by citizens to assess the fairness of legal procedures. *Law & Society Review*, (22(1)), 103-136.
9. Tyler, T.R. & Hou, Y.J. (2002). *Trust in the law: Encouraging public cooperation with the police and courts*. New York, NY: Russell Sage.
10. Mastrofski, S. (1999). *Policing for people. Ideas in American Policing*. Washington, DC: Police Foundation.
11. Roth, J.A., Ryan, J.E., Gaffigan, S.J., Koper C.S., Moore, M.H., Roehl, J.A. & Thacher, D. (2000). *National evaluation of the COPS Program – Title 1 of the 1994 Crime Act*. Washington, DC: U.S. Department of Justice, National Institute of Justice.
12. Gill, C.E., Weisburd, D. Telep, C.W, Vitter, Z. & Bennett, T. (2014). Community-oriented policing to reduce crime, disorder, and fear and increase satisfaction and legitimacy among citizens: A systematic review satisfaction in neighborhoods. *Journal of Experimental Criminology*, (10), 399-428.
13. Telep, C. & Weisburd, D. (2012). What has been learned from systematic reviews in policing? In D. P Farrington & D. Weisburd (Eds.), *Systematic reviews in criminology: What have we learned*? New York, NY: Springer.
14. Goldstein, H. (1979). Improving policing: A problem-oriented approach. *Crime & Delinquency*, (24), 236-258.
15. Goldstein, H. (1990). *Problem-oriented policing*. New York, NY: McGraw-Hill.
16. Eck, J. & Spelman, W (1987). *Problem-solving: Problem-oriented policing in Newport News*. Washington, DC: Police Executive Research Forum.
17. Weisburd, D., Telep, C, Hinkle, J. & Eck, J. (2008). Is problem-oriented policing effectiveness in reducing crime and disorder. *Criminology & Public Policy*, (9(1)), 139-172.
18. Jones, G. (2007). *The use of CIS, crime analysis, and information sharing to enhance gang intervention strategies: A regional perspective* (unpublished). Washington, DC: Police Foundation.
19. Jones, G. & Malina, M. (Eds.) (2011). *Crime analysis case studies*. Washington, DC: Police Foundation and U.S. Department of Justice, Office of Community Oriented Policing Services.
20. Problem-Oriented Policing. Better Policing Toolkit. RAND. Retrieved from https://www.rand.org/pubs/tools/TL261/better-policing-toolkit/all-strategies/problem-oriented-policing.html
21. Santos, R.B. (2014). The Effectiveness of Crime Analysis for Crime Reduction: Cure or Diagnosis? *Journal of Contemporary Criminal Justice*, (30 (2)), 147-168. Retrieved from https://doi.org/10.1177/1043986214525080
22. Bratton, W. (1998). *The turnaround: Flow America top cop reversed the crime epidemic*. New York: Random House.
23. Bratton, W. & Knobler, R. (1998). *The turnaround: How America top cop reversed the crime epidemic*. New York: Random House.
24. Kelling, G. & Bratton, W. (1998). Declining crime rates: Insiders' views of the New York City story. *Journal of Criminal Law and Criminology*, (88 (4)), 1217-1232.
25. Shane, J. (2007). *What every chief executive should know: Using data to measure police performance*. Flushing, NY: Looseleaf Law Publications.
26. Wakefield, A. & Fleming, J. (2009). *The SAGE dictionary of policing*. Thousand Oaks, CA: Sage Publications.

27. Weisburd, D., Mastrofski, S., McNally, A. M., Greenspan, R. & Willis, J. (2003). Reforming to preserve: Compstat and strategic problem solving in American policing. *Criminology & Public Policy*, (2(3)), 421-456.
28. *First Look at New York City's New CompStat 2.0: Eight Crime Trends in Brooklyn*. Retrieved from https://brooklyneagle.com/articles/2016/02/24/first-look-at-nycs-new-compstat-2-0-eight-brooklyn-crime-trends/
29. Chainey, S. & Ratcliffe, J. (2005). *CIS and crime mapping*. Chichester, West Sussex, UK: John Wiley & Sons, Ltd.
30. White, M. (2009). *Jacksonville Sheriff's Office mapping with text analysis*. Crime Mapping News, (8 (1)). Washington, DC: Police Foundation.
31. *National Highway Traffic Safety Administration* (2009). Data-driven approaches to crime and traffic safety: Operational guidelines. Washington, DC: U.S. Department of Transportation, National Highway Traffic Safety Administration. Retrieved from http://www.nhtsa.gov/staticfiles/nti/ddacts/811185_ DDACTS_OpGuidelines.pdf
32. Perry, W L., Mdnnis, B., Price, C., Smith, S., &r Hollywood, J. (2013). Predictive policing: The role of crime forecasting in law enforcement operations. Washington, DC: Rand Corporation.
33. Uchida, C. (2009, November). *A national discussion on predictive policing: Defining our terms and mapping successful implementation strategies* (Discussion Paper). Washington, DC: U.S. Department of Justice, National Institute of Justice.
34. Pearsall, B. (2010, June). Predictive policing: The future of law enforcement. *NIJ Journa*l, (266). Washington, DC: U.S. Department of Justice, National Institute of Justice.
35. Olligschlaeger, A. (2015). *Crime forecasting on a shoestring budget*. Crime Mapping and Analysis News, Issue 2. Washington, DC: Police Foundation.
36. Clarke R., &r Eck, J. (2005). *Crime analysis for problem solvers in 60 small ste*ps. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.
37. Peterson, M. (2005). *Intelligence-led Policing: The new intelligence architecture*. Washington, DC: U.S. Department of Justice, Bureau of Justice Assistance.
38. Користін О.Є., Пефтієв Д.О., Пеньков С.В., Некрасов В.А. Довідник керівника поліції – поліцейська діяльність, керована розвідувальною аналітикою /ILP. Київ: «Видавництво Людмила», 2019. 120 с.

DOI: https://doi.org/10.36486/978-966-2310-66-5-6

Традиційно вважається, що правоохоронна діяльність не піддається змінам, однак у сучасних умовах вона майже постійно адаптується до тиску як внутрішніх, так і зовнішніх факторів.

Dr. Jerry H. Ratcliffe

РОЗДІЛ 6
Філософія ILP – концепція Джеррі Ретклiффа

Олександр Користін
Богдан Денисенко

Поліцейська діяльність, керована аналітичною розвідкою (*Intelligence-led Policing, ILP*) – це сучасна модель, яка передбачає інкорпорування розвідувальної аналітичної функції в загальну місію правоохоронної системи.

> *Комплексне завдання – прогнозування ризиків та вплив на діяльність – передбачає комбінування аналізу й процесу прийняття рішень та створює додаткові виклики для фахівців.*

Проактивна поліцейська діяльність, закладена в поняття ILP, вимагає від аналітиків, політиків, керівників правоохоронних органів та інших осіб, що відповідають за прийняття рішень, нових навичок і компетенцій. Це також означає необхідність обізнаності осіб, що приймають рішення, про можливості проведення аналізу та про те, як використовувати його результати.

Модель ILP включає в себе чіткі організаційні та управлінські структури, в тому числі механізми прийняття рішень і постановки завдань на місцевому, регіональному та національному рівнях, а також певні процеси співпраці й комунікації між правоохоронними органами на місцевому рівні та в рамках міжнародного співробітництва. Водночас,

> *більш ефективне управління даними та інформацією є важливою перевагою ILP для сучасних правоохоронних органів.*

Існують різні й навіть суперечливі трактування поняття ILP. Деякі вважають, що ILP відноситься до оцінювання загроз та ризиків, у той час як інші стверджують, що ця модель спрямована на збір даних та інформації. Хоча такі точки зору важливі для розуміння значущості та опису основних компонентів системи, їх недостатньо для викладу всеохоплюючої концепції ILP.

Але перш ніж перейти до розгляду ILP, необхідно прояснити кілька ключових понять. Етимологічна характеристика терміна intelligence у контексті сутності сучасної моделі безпекової діяльності (*див.* – розділ 5) потребує відходу від однозначного елементарного перекладу, і обґрунтовує позицію більш широкого тлумачення як АНАЛІТИЧНА РОЗВІДКА.

ДАНІ, ІНФОРМАЦІЯ, ЗНАННЯ

Мають місце певні суперечливі погляди та нечітке розуміння значень ключових термінів (рис. 6.1).



Рисунок 6.1. Контекстний зв'язок понять у моделі аналітичної розвідки [1, с. 70-74]

> *«Відсутність чіткості та загального розуміння термінології та процесів кримінальної розвідки перешкоджає обміну інформацією між поліцейськими агенціями». Міжнародна асоціація керівників поліції (2002)*

Після вивчення документів, опублікованих UNODC [2], ІНТЕРПОЛ [3] та Європейським Союзом (ЄС) [4], а також академічної літератури [1, с.70-74], у виданні «OSCE Guidebook Intelligence-Led Policing» [5] зроблено акцент на такому загальноприйнятому використанні визначень вищезгаданих концепцій:

> ***ДАНІ** – це необроблені й неінтерпретовані результати спостережень і вимірювань.*

Це спостереження, які можемо зробити щодо злочинів або загроз. Приклади містять у собі особливості злочинної діяльності, що легко піддаються кількісній оцінці, наприклад, повідомлення про злочини та інші статистичні дані, бази даних про правопорушників, де інформація була попередньо запрограмована, класифікована та введена в систему. Дані – це прості спостереження, необмежені додатковими змінами, висновками чи думками. Дані можуть відноситись до місць злочину, характеристик способів вчинення злочину, зброї та підозрюваних.

> ***ІНФОРМАЦІЯ** – це дані, вміщені в контекст і осмислені, що надає їм більшу актуальність і значущість.*

Це дані з більшою релевантністю. Інформація наділена сенсом і контекстом, і може бути неструктурована за своїм характером. Наприклад, інформація зі стенограми прослуховування може продемонструвати більш глибоке розуміння відносин між організатором злочину та співучасниками. Для введення в базу даних інформація має бути подана у контексті й оцінена фахівцем та розподілена відповідно до систем, запроваджених аналітичними підрозділами. Тому інформацію важче передати без певної загальної одиниці вимірювання, що має сенс для того, хто передає, та того, хто приймає.

> ***ЗНАННЯ** – це інформація після її тлумачення і засвоєння. Коли людина додає власний досвід до інформації, вона стає знанням.*

У сучасних безпекових системах поняття «знання» увійшли до мови операційної діяльності. Ще донедавна це був більш екзотичний термін, що вживався ученими для обговорення концепцій управління інформацією, зараз є одним із останніх нововведень.

Національна розвідувальна модель Великої Британії (The National Intelligence Model (NIM)) використовує терміни «активи знань» та «продукти знань», а поліцейські Норвегії застосовують модель поліцейської діяльності на основі знань. Знання мають цінність саме тому, що фахівець дає інформаційний контекст, тобто певну конкретну інтерпретацію. Знання складно структурувати, зберігати або поширювати, вони також більш нематеріальні, ніж дані. Знання є надзвичайно вразливими щодо специфіки організаційного та культурного середовища, а за умови відсутності адекватних інформаційних систем іноді мають потенційно руйнівні наслідки у випадку їх передачі.

Таким чином, *важливість того чи іншого підрозділу в організаційній структурі визначається не репутацією, а «знаннями». У свою чергу в умовах ILP звичайним, але центральним функціональним напрямом поліції стає нарощування потенціалу від «знань» до аналітичної розвідки.*

Продукти знань створюють умови щодо розуміння поведінки злочинця, але продукти аналітичної розвідки мають генерувати дії, конкретні управлінські дії у сфері державної безпеки. Тобто не завжди «знання» автоматично переходять у розряд управлінських рішень. Так само й управлінські рішення не завжди покладаються на аналітичну розвідку. Ця проблема не є унікальною.

> ***Аналітична розвідка (intelligence)** – це дані, інформація та знання, які були оцінені, проаналізовані та представлені у форматі прийняття рішень для діяльнісно-орієнтованих цілей.*

Для багатьох аналітиків розрив між продукуванням знань та продукуванням результату аналітичної розвідки є суттєвим. Щоб розвинути глибоке розуміння проблеми безпеки та загроз, інформація має бути поміщена в контекст та організована таким чином, щоб посадові особи, які приймають рішення, мали уявлення та робили висновки з наявної колективної мудрості. Знання можуть поглиблювати уявлення та розуміння, але вони повинні бути структуровані таким чином, щоб допомогти особам, які приймають рішення, розробляти план дій.

***Приклад.** До поліцейської бази даних місцевої поліцейської дільниці вносяться дані про квартирні крадіжки. Ці комп'ютерні записи є даними. Коли аналітик, обробляючи та класифікуючи дані, виявляє*

нову закономірність крадіжок у районі, це стає інформацією. По суті, необроблені дані були достатньо осмислені для виявлення закономірностей. Якщо згодом аналітик поділиться цією інформацією зі слідчим та обговорить її, то розуміння та засвоєння зробить з цієї інформації знання. Збираючи та аналізуючи додаткові дані та інформацію, слідчий та аналітик можуть побудувати картину, яка, безперечно, не буде повною, але матиме достатньо матеріалу для підкріплення гіпотез та формулювання можливих наслідків. Аналітик та слідчий складають звіт про результати кримінального аналізу та викладають його старшій посадовій особі. Вона приймає рішення про початок розслідування та здійснення спецзаходів з орієнтацією на грабіжників на основі аналітичного продукту від аналітика та детектива [5].

Стратегічні переваги, засновані на даних, інформації, знаннях та аналітичній розвідці, підвищують рівень безпеки та ефективність правоохоронних органів у запобіганні правопорушенням, а також припиненні діяльності злочинних угруповань. Але мати дані, інформацію, знання та аналітичну розвідку недостатньо. Для управління аналітичним розвідувальним процесом та його максимального використання необхідно сформувати відповідну структуру або модель, так само як і для збору, обробки та використання даних й аналітичної розвідки суворо відповідно до національних законів та міжнародних стандартів у галузі прав людини.

РІВНІ АНАЛІТИЧНОЇ РОЗВІДКИ

Існують різні підходи до визначення рівнів аналітичної розвідки, але традиційний підхід щодо визначення аналітичної розвідки має три площини (рис. 6.2):



Рисунок 6.2. Рівні аналітичної розвідки – INTELLIGENCE

> ***ТАКТИЧНИЙ РІВЕНЬ** – підтримка безпосередньої діяльності слідчого та оперативного працівника, детектива, конкретного розслідування кримінального провадження, негласних слідчих розшукових дій, спеціальних операцій та оперативно-розшукових заходів тощо з метою забезпечення та досягнення визначеної мети.*

Тактичний рівень є найпоширенішим застосуванням аналітичної розвідки у системі правоохоронної діяльності.

Поряд із цим, має місце хибне визначення пріоритету застосування тактичного рівня та вимоги керівників підрозділів щодо концентрації аналітиків на тактичних результатах і на підтримці розслідувань, а не на аналізі основних безпекових проблем.

> ***ОПЕРАТИВНИЙ РІВЕНЬ** – допомога управлінню для досягнення оперативних цілей; підтримання регіональних керівників, територіальних підрозділів у плануванні діяльності щодо зменшення масштабів злочинності та розгортання ресурсів для досягнення оперативних цілей.*

Існують підрозділи та деякі аналітики, які не визнають арену оперативного рівня, однак це одна із найбільш швидкозростаючих сфер управління розвідувальною інформацією у межах безпекової діяльності. Знаходячись між сфокусованою на правопорушниках тактичною ареною та стратегічним рівнем щодо формування стратегії, політики та довгострокових планів, оперативний INTELLIGENCE, який може сприяти зниженню масштабів загроз у регіонах та плануванню відповідних ресурсів, безсумнівно, є ключовим компонентом.

> ***СТРАТЕГІЧНИЙ РІВЕНЬ** – забезпечує прийняття рішень, розробку політики, планування та визначення пріоритетів; розподіл ресурсів поліції; та, із врахуванням видів злочинності, визначає відповідний підхід діяльності поліції; спрямовується на забез-*

> *печення уявлення щодо загроз уразливості, ризиків та можливостей щодо діяльності (оцінка загроз та ризиків) у сфері безпеки, розуміння тенденцій та системи причинно-наслідкових зв'язків, а також є внеском у розроблення широких стратегій щодо безпекової політики та використання ресурсів.*

Стратегічний рівень аналітичної розвідки завжди перебував у тіні щодо легітимності його застосування. Стратегічний рівень має справжні організаційні наслідки, є базисом і пронизує весь аналітичний процес. Він також має потенціал бути найважливішим аспектом у системі аналітичної розвідки через здатність стратегічних продуктів впливати на загальну безпекову стратегію та рішення щодо використання ресурсів.

Стратегічний рівень аналітичної розвідки не є терміном, пов'язаним з винятково загальнодержавним безпековим аспектом, він також застосовується до процесу планування та розподілу ресурсів на кожному структурному рівні у межах безпекової політики.

ПРОАКТИВНІСТЬ МОДЕЛІ ILP

Намір передбачення конкретної загрози краще було б замінити метою визначення майбутніх поведінкових патернів (зразків, шаблонів, моделей, систем) для посилення на проактивному компоненті. Перехід до формату INTELLIGENCE був частково простимульований бажанням посилити проактивний підхід, який використовують для ефективного запобігання деструктивним явищам замість традиційного реагування на вчинені протиправні дії. Для того, щоб вжити власне запобіжні заходи, і потрібен проактивний підхід. Проактивність, натомість, вимагає наявності компонента передбачуваності, якщо характеризуємо загрозу. Якщо діяльність є унікальною за своєю природою, ми навряд чи матимемо можливість визначити певні майбутні події через те, що нам потрібна «історія», аналогічні інциденти, зв'язок між якими можливо простежити, встановивши певну залежність.

Послідовність: *запобігання, проактивність, передбачуваність та залежність* (рис. 6.3) визначає ідентифікацію залежності (відповідних патернів) як передумову ефективному запобіганню загрозі та є основним компонентом INTELLIGENCE.



Рисунок 6.3. Ланцюг ключових патернів моделі ILP [5]

Незважаючи на можливість виникнення певних відхилень у короткостроковій перспективі, більшість тенденцій та проблем залишаються незмінними до моменту прийняття рішення про вжиття дієвих заходів. Значення патернів є особливо важливим, вони є «ядром» так званого першого закону INTELLIGENCE:

> *найбільш чітким індикатором потенційної злочинної діяльності є аналогічні дії, що вчиняються зараз.*

Особи, які проявили певні можливості та скористалися ними, будуть продовжувати доти, поки їх не зупинять, і таким чином можливим стане визначення патерну конкретної повторюваної діяльності. Стратегічний менеджмент патернів (обставини інцидентів та поведінкова специфіка) буде оптимальним форматом, на відміну від індивідуальних розслідувань.

Суто з аналітичного погляду, ідентифікація патернів (обставини інцидентів та поведінкова специфіка) є першим кроком на шляху до запровадження проактивного підходу.

> *Навіть дескриптивний (описовий) аналіз патернів щодо вчинених у минулому злочинів може бути використаний для прогнозування майбутньої динаміки.*

Також існує думка, що безперервність ланцюга подій, які характеризують досліджуваний патерн, може бути порушена лише вжиттям відповідних заходів.

Інша складова комбінованого процесу прогнозування в контексті INTELLIGENCE – вплив на тих, хто приймає рішення. Базовою у цьому випадку є аксіома аналітичної розвідки:

> *аналітична розвідка, що не впливає на мислення того, хто приймає рішення, не є справжньою аналітичною розвідкою.*

Водночас жодним чином не применшується цінність підтримки процесу розслідування, надання консультацій та іншої, не менш важливої роботи, яку виконують аналітики, але аналітична розвідка – це процес формування знань.

ЗМІСТ ОСНОВНИХ ЕЛЕМЕНТІВ, ЩО ХАРАКТЕРИЗУЮТЬ АНАЛІТИЧНУ РОЗВІДКУ

Урахування помилок, або некоректного розуміння основних функцій та специфіки аналітичної розвідки, формує зміст основних елементів, що характеризують діяльність підрозділів кримінального аналізу:

Аналітична розвідка є спеціалізацією – її слід розглядати як окрему спеціальність; залучати до її виконання слід незаангажованих осіб, які забезпечать відсутність конфлікту інтересів та застосування результатів для підтримки відповідної проактивної політики, генеруючи підкріплений надійною інформацією продукт.

Аналітична розвідка є критично важливою – для забезпечення точності даних необхідно систематично ставити під сумнів традиційні переконання. Сприймати інформацію без перевірки відповідного бекграунду, надійності джерела чи висновків, які надаються, означає підривати саму основу процесу.

Аналітична розвідка має кількісний вимір – будь-яка правоохоронна діяльність, результати якої неможливо оцінити за кількісними показниками, є неефективною. Аналітична розвідка – не виняток; під час виконання завдань із запобігання чи мінімізації впливу організованої злочинності результати будь-якої програми повинні бути легко інтерпретованими та вимірюваними.

Аналітична розвідка не потребує публічності – основним завданням цих підрозділів є запобігання злочинам, але водночас ніде не закріплено обов'язок щодо інформування громадськості про використання відповідних стратегій і технік. Метою утримання відповідної інформації від розголосу є уникнення певних конфліктів.

Аналітична розвідка часто спрямована на вирішення тих проблем, які ігноруються іншими – оскільки аналітичні підрозділи спрямовані на проактивний підхід, вони мають чіткий обов'язок ідентифікувати проблеми, які виникають; ці проблеми зазвичай ігноруються чи залишаються поза увагою інших.

Аналітична розвідка вимагає уваги до деталей – якщо йдеться про боротьбу з організованою злочинністю, деталі є надважливими, слід уникати узагальнень та оцінки діяльності злочинців на основі загальноприйнятих критеріїв. Інакше кажучи, увага до деталей, які обґрунтовують причини надання злочинній організації більш високої пріоритетності, підкреслює справжній характер аналітичної розвідки.

Аналітична розвідка є мистецтвом «фільтрування» необроблених потоків даних для отримання аналітичного продукту. Важливішим є, можливо, усвідомлення того, що пропорційна оцінка загроз є необхідною для забезпечення вжиття оптимальних заходів (без перебільшення загрози чи, навпаки, її применшування). Не на всі загрози слід реагувати однаково – важливо розмежовувати реальні від хибних; досягти цього можливо лише шляхом проведення ретельного аналізу та за умови наявності відповідного досвіду і знань.

ОРГАНІЗАЦІЙНА МОДЕЛЬ ДЛЯ ILP

Сутність взаємозв'язку між ключовими учасниками моделі ILP (безпековим середовищем, аналітиком та особою, відповідальною за прийняття рішень) розкриває модель «4-х і» (рис. 6.4, 6.5).

i →		intent	Намір
i →		interpret	Інтерпретація
i →		influence	Вплив
i →		impact	Імпульс впливу

Рисунок 6.4. Модель «4-х і» [1, с. 70-74]

Для того щоб повністю реалізувати потенціал ILP, необхідно, щоб всі чотири компоненти «**і**» функціонували належним чином. Модель базується на взаємозв'язку між аналітичною розвідкою та особами, які приймають рішення [1, с. 70-74]:

по-перше, *особи, відповідальні за прийняття рішень, визначають завдання, направляють, консультують аналітиків і керують ними, мають бути переконаними в тому, що їхні наміри роз'яснені і зрозумілі;*

по-друге, *аналітики інтерпретують безпекове середовище;*

по-третє, *аналітики впливають на осіб, які приймають рішення, за допомогою результатів аналізу;*

по-четверте, *на основі цих висновків особи, які приймають рішення, впливають на середовище за допомогою стратегічного управління, планів дій, розслідувань і операцій тощо.*

За цією моделлю аналітик повинен не лише активно інтерпретувати специфіку безпекового середовища, а й впливати на прийняття рішень. Це вимагає не лише ідентифікації відповідної особи чи групи, які мають потенціал протидіяти визначеній проблематиці, але також врахування найбільш оптимальних способів впливу на їхню ментальність.



Рисунок 6.5. Організаційна модель на основі 4-і [1]

Друге завдання завжди простіше виконати, якщо особа, відповідальна за прийняття рішень, «йде на контакт» і сприймає позитивно філософію ILP. Більше того, ця схема показує нам, що під час взаємодії з цими особами аналітики повинні усвідомлювати необхідність вироблення адекватних рекомендацій щодо того, як ефективно впливати на кримінальне середовище.

> *Необхідно зрозуміти, що формування політики з урахуванням аналітичної розвідки – це не просто конкретний метод чи засіб, а, швидше, певна зміна у культурі «виробництва», що відкриває шлях до змін загалом.*

Маючи потенціал для здійснення такого широкого впливу, нова модель, безсумнівно, передусім повинна органічно вписуватися в загальну систему та враховувати потреби усіх учасників процесу.

Крім того, будь-яка політика чи модель має працювати у тандемі з іншими відповідними регулюючими законодавчими актами та методологіями.

Це означає, що хоча принципи формування політики ILP можуть залишатися в усьому світі тими самими, у підходах до конкретної діяльності все одно неминуче існуватимуть розбіжності за географічними, організаційними, культурними чи політичними ознаками. З одного боку, ці розбіжності обов'язково обмежуватимуть універсальність будь-якого підходу до формування політики ILP; але з іншого – достатньо корисною буде можливість вивчати різні підходи до формування політики ILP та оцінювати їх ефективність.

На думку багатьох аналітиків, одним із головних передвісників прийняття ILP певною установою є усвідомлення нею неадекватності наявних аналітичних, розвідувальних та організаційних методологій, оскільки формування політики з урахуванням аналітичної розвідки передбачає не просто створення нової політики, а зміну організаційної культури, потребує чіткої стратегії імплементації, яка спирається на практику та прагматизм.

ПРИЙНЯТТЯ РІШЕНЬ ТА ЛІДЕРСТВО

Для того, щоб ILP модель запрацювала на повну силу, аналітична розвідка повинна бути інкорпорована у процес планування діяльності органу. Передумовою успішної імплементації є відповідний рівень структурування та «зрілості» середовища відповідальних за рішення осіб.

Практика показує, що проблем безліч: у багатьох підрозділах процес прийняття управлінських рішень нагадує лабіринт: начальники, заступники (управлінь, відділів), керівники середньої ланки та працівники, що мають певну свободу для прийняття важливих рішень, але не мають можливості звернутися до аналітиків по допомогу, щоб хоча б частково зрозуміти сутність проблеми.

Навіть коли визначені чіткі інструкції щодо здійснення комунікації та прийняття рішень, вони не гарантують, що рішення прийматимуться на відповідному стратегічному рівні та базуватимуться на оцінюванні їх ефективності.

Занадто часто керівники надміру покладаються на власні упередження замість того, щоб брати до уваги поточну оцінку проблем.

> *Сильні лідери можуть бути на 100% продуктивними в індивідуальному плані, але програвати, коли йдеться про стратегічне мислення.*

ПЕРЕВАГИ ПОЛІЦЕЙСЬКОЇ ДІЯЛЬНОСТІ, КЕРОВАНОЇ АНАЛІТИЧНОЮ РОЗВІДКОЮ

У правоохоронній діяльності аналітична розвідувальна робота відіграє непересічну роль. Для того чи іншого правоохоронного підрозділу ефективне використання інформаційно-аналітичного процесу може означати успіх або поразку. У наш час, коли наявна багата інформація видається нерідко суперечливою та нечіткою, аналітична розвідка може вказати шлях до розробки ефективної політики.

Ефективна аналітична розвідка значно впливає на спроможність тієї чи іншої правоохоронної установи щодо протидії кримінальним угрупованням. Аналітична розвідка забезпечує правоохоронну установу інформацією та рекомендаціями, що дозволяють їй ефективно використовувати свої ресурси. Вона надає правоохоронним органам можливість виявляти та розуміти діяльність кримінальних угруповань, що діють на їхній території.

Після виявлення кримінальних угруповань та встановлення їхніх звичок правоохоронні органи можуть розпочинати оцінку поточних тенденцій щодо злочинності та прогнозувати й запобігати вчиненню правопорушень.

Аналітична розвідка надає інформацію, з урахуванням якої мають ухвалюватися рішення та визначатися відповідні об'єкти (окремі особи чи кримінальні угруповання) розслідувань. Хоча аналітична розвідка може використовуватися для допомоги досудовим розслідуванням, проведенню негласних слідчих розшукових дій та переслідуванню злочинців, вона також

> *забезпечує правоохоронні органи можливістю ефективного використання своїх ресурсів, управління бюджетами.*

Різні практики та коментатори намагалися прив'язати правоохоронну діяльність, керовану аналітичною розвідкою, до концептуальних рамок поліцейської діяльності, які існують на сьогодні. Проте якщо правоохоронна діяльність, керована аналітичною розвідкою, є справді новою пара-

дигмою правоохоронної діяльності, то її слід визнати суттєво відмінною від попередніх моделей правоохоронної діяльності.

Науковці присвячують цілі книги з'ясуванню конкретних стилів правоохоронної діяльності, і багато поліцейських департаментів оперують моделями, які є гібридами цих різних підходів. Серед них спостерігається значна невизначеність щодо поліцейської діяльності, керованої аналітичною розвідкою. Але необхідно розуміти, що

> *є немало того прогресивного та інноваційного, що виділяє поліцейську діяльність, керовану аналітичною розвідкою, як більш ефективну, перспективну та раціональну щодо використання державних ресурсів.*

Модель ILP містить чіткі організаційні та управлінські структури, у тому числі механізми прийняття рішень та постановки завдань на місцевому, регіональному та національному рівнях, а також певні процеси співробітництва та комунікації між правоохоронними органами на місцевому рівні та в рамках міжнародного співробітництва.

ПОМИЛКИ ЩОДО СПРИЙНЯТТЯ МОДЕЛІ ILP

Уся аналітична розвідка, враховуючи навіть опис злочинів, учинених у минулому, створює певну проєкцію безпекового середовища у майбутньому. Для підтвердження цього необхідним є вилучення одного з видів діяльності, який досить часто некоректно визначають як аналітичну розвідку – підтримка розслідування (дії, що виконуються з метою збору достатньої кількості доказів для висунення обвинувачення), яка є цінною в контексті забезпечення ефективної діяльності поліції, але вона відіграє другорядну роль і не є власне розвідувальною діяльністю, незалежно від того, якими є функціональні обов'язки осіб, що її забезпечують.

По-перше, діяльність аналітиків переважно спрямована на застосування наявних знань для прогнозування потенційних ситуацій; цей процес не є вже сталим та поширеним, часто аналітики та їхні керівники задоволені результатами звітів про наявні тенденції та динаміку загроз, абсолютно без будь-яких прогнозів; однак прогнозування є дуже важливим для тих, хто приймає рішення, адже вони також виконують і функцію ризик-менеджерів, на яких покладено відповідальність за розподіл ресурсів.

По-друге, керівники дуже часто доручають підлеглим неможливі для виконання завдання. У цьому випадку вони не в змозі адекватно сформулювати свої вимоги та наміри, за звичкою шукають «правильні відповіді», такі собі ситуативні проєкції конкретної дати, часу та місця вчинення потенційного правопорушення тощо. Якщо підлеглі дають менший за визначений обсяг інформацію – це вважається провалом.

ПОМИЛКОВІ ТВЕРДЖЕННЯ ЩОДО ФУНКЦІЙ ILP

Аналітична розвідка є унікальною діяльністю, до якої залучаються професіонали високого рівня, які можуть визначити, що саме може правоохоронний орган вирішувати самостійно у рамках своїх повноважень, а що – ні. Спроможність правильно формулювати і легітимізувати функції аналітичної розвідки є надзвичайно важливою. Однак, слід проаналізувати певні помилкові твердження:

Помилка 1. *Будь-які підрозділи можуть бути залученими до аналітичної розвідувальної діяльності.*

Для виконання таких завдань необхідною є відповідна спеціалізація – комплекс знань та навичок, що виходять за межі стандартної підготовки працівників. Не всі підрозділи мають відповідні ресурси для виконання таких функцій, у більшості структур їх критично бракує. Складність завдань вимагає залучення осіб з унікальними навичками та особистими якостями. Для розвідувальних аналітичних служб типовим є застосування проактивного підходу, проте без надмірного тиску та втручань.

Помилка 2. *Аналітичні розвідувальні функції може виконувати будь-який працівник.*

Не всі правоохоронні органи мають відповідний потенціал та можливості залучати до виконання розвідувальних функцій винятково кваліфікований та досвідчений персонал, який може забезпечити дотримання всіх методологічних, законодавчих та етичних вимог.

Помилка 3. *Аналітичні розвідувальні системи є, по суті, інформаційними системами.*

Дуже часто, коли необхідно в будь-який спосіб уникнути вживання терміна «розвідка», правоохоронні органи натомість застосовують визначення «інформаційна система». АЛЕ: по-перше, розвідувальна

аналітична робота спрямована на виконання низки функцій, які не є притаманними інформаційним системам. Наприклад, завданням підрозділу кримінального аналізу є своєчасне представлення певного «аналітичного продукту» для подальшого використання; інформаційні системи існують для виконання певних операцій з даними – водночас дані не обов'язково є придатними для подальшого використання, своєчасно поданими або ретельно проаналізованими.

Ще одна відмінність: діяльність підрозділів кримінального аналізу є безперервним, динамічним процесом (трансформація інформації у знання), в той час як всі інформаційні системи є статичними за природою. Саме тому слід обережно вживати визначення «інформаційна система» у контексті аналітичної розвідки.

Помилка 4. *Аналітична розвідувальна діяльність є лише правильною підготовкою.*

Унікальна природа цієї діяльності дає змогу припустити, що прогнозування є передумовою для реалізації будь-якої життєздатної аналітичної розвідувальної програми. Підготовка потребує не лише наявності опрацьованої інформації.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Jerry H., Ratcliffe (2016). *Intelligence-Led Policing. Second edition.* New York: Routledge.
2. *Criminal Intelligence:* Manual for Analysts (2011). Vienna: UNODC. New York: United Nations.
3. INTERPOL. Criminal Intelligence Analysis. *Fact Sheet*. 2014. Retrieved from https://www.interpol.int/
4. Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. *Official Journal of the European Union*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006F0960
5. *OSCE Guidebook Intelligence-Led Policing* (2017). TNTD/SPMU Publication. Series Vol. 13. Vienna.

DOI: https://doi.org/10.36486/978-966-2310-66-5-7

«...майже неможливо обговорювати концепцію поліцейської діяльності, керованої аналітичною розвідкою, не посилаючись на National Intelligence Model (NIM)».

Dr. Jerry H. Ratcliffe

РОЗДІЛ 7
Актуалізація аналітичної розвідки в національній правоохоронній моделі

Юрій Кардашевський

Упроваджуючи модель правоохоронної діяльності, керованої аналітичною розвідкою (*Intelligence-led Policing – ILP*), необхідним є сприйняття її не лише у якості аналітичного процесу, а й у якості нової філософії правоохоронного менеджменту. Українські правоохоронні органи вже застосовують певні аспекти моделі ILP, але в цілому ще багато не вирішених проблем щодо її імплементації [1]. Обґрунтованість тих чи інших рішень щодо упровадження ILP об'єктивно передбачає глибоке вивчення зарубіжного досвіду, врахування проблемних питань, визначення усього комплексу завдань та пріоритетів щодо упровадження в перспективі.

Перш за все, звертає на себе увагу те, що у правоохоронному середовищі немає загальноприйнятого визначення поліцейської діяльності, керованої аналітичною розвідкою. Спробою започаткування була публікація Міжнародної асоціації аналітиків правоохоронних органів (*International Association of Law Enforcement Intelligence Analysts - IALEIA*):

> *«Поліцейська діяльність, керована аналітичною розвідкою, передбачає збір і аналіз інформації для створення остаточного аналітичного продукту, призначеного для інформування поліції в процесі прийняття рішень як на тактичному, так і на стратегічному рівнях» [2].*

Група Global Justice розширила це, щоб більш широко визначити мету: «*ILP – це імплементоване виконання циклу аналітичної розвідки для підтримки проактивного прийняття рішень щодо розподілу ресурсів і запобігання злочинності*» [3, с. 4].

Водночас д-р Джеррі Ретклiфф стверджував, що ILP має вищу мету як

> *«... бізнес-модель і філософія управління, де аналіз даних і кримінальна розвідка є ключовими для об'єктивності системи прийняття рішень, що сприяє зниженню злочинності та проблем її усуненню, руйнуванню і запобіганню як через стратегічне управління, так і ефективні стратегії правозастосування, що спрямовуються на небезпечних злочинців» [4].*

Хоча існує певна неоднозначність у визначенні ILP [4], ця концепція загалом зосереджена на аналізі та використанні розвідувальної інформації щодо злочинів для систематичного спрямування зусиль на зниження та запобігання злочинності [5; 6; 7]. Водночас

> *ILP робить аналітичну розвідку ключовим визначальним фактором для розподілу ресурсів по всьому відомству [5].*

У 1994 році у Великій Британії вперше було впроваджено поліцейську діяльність, керовану аналітичною розвідкою. Її метою було «*зменшення рівня злочинності та підвищення громадської безпеки*» [8, с. 6]. Поліція графства Кент, перебуваючи під тиском щодо необхідності зниження злочинності та зіткнувшись зі скороченням фінансування, запровадила такого роду новацію, в результаті якої протягом трьох років відбулося зниження злочинності на понад 22 відсотки [8, с. 7].

Кентська модель була запроваджена як «*цілісна система ILP*» [9, с. 455] і привернула до себе позитивну увагу, а пізніше була описана як «*наймасштабніший і найвпливовіший*» проект ILP, продемонстрований в Англії та Уельсі [10, с. 313].

Річард Андерсон у своїй праці «Intelligence-led Policing: A British Perspective», видавництва IALEIA, ключовими моментами ILP визначав:

> *«Створення картинки ключової кримінальної активності; розуміння та візуалізація мережі наркоторговців у певному місці, наприклад, зосереджує аналітичний пошук на визначених потребах, допомагає у виборі цілей для максимального руйнування злочинності, пропонує можливості для вербування інформаторів і дозволяє розробляти гіпотези щодо майбутньої кримінальної активності, базуючись на запланованій правоохоронній діяльності» [8, с.7-8].*

Величезний вплив на усі правоохоронні органи та на усіх рівнях США мали теракти в Нью-Йорку, Вашингтоні та Пенсильванії у 2001 році. Менш ніж через 60 днів після терактів 11 вересня Міжнародна асоціація начальників поліції (IACP) провела свою щорічну конференцію в Торонто (Канада). IALEIA брала участь у цій конференції разом з багатьма іншими професійними поліцейськими організаціями. Під час конференції проводилися зустрічі та обговорювалися питання щодо правоохоронних заходів у відповідь на терористичний виклик [11]. Основна ідею саміту стосувалася обміну аналітичними розвідувальними даними.

Зазначену ідею було розвинуто у березні наступного року в Арлінгтоні (штат Вірджинія). Участь взяли понад 100 поліцейських, які цікавилися питаннями аналітичної розвідки. Основні презентації були представлені щодо британської моделі ***National Intelligence Model (NIM)***, яку у подальшому було використано для розвитку відповідної американської моделі. Сутність британської моделі полягала у тому, щоб безпосередньо пов'язати планування заходів з операційними результатами. Вона передбачала довгострокові переваги інтегрованої системи розвідки, поєднуючи розвідувальні, профілактичні та правоохоронні дії на місцевому, регіональному та національному рівнях [12, с. 12].

У «блакитній книзі» Національної служби кримінальної розвідки (*National Criminal Intelligence Service* – NCIS) [12, с. 2] стверджується, що NIM «*забезпечує ясність і стандарти для розвідувальної діяльності*» і дозволяє переглянути «*розвідувальні системи і ввести більшу суворість у процес прийняття управлінських рішень*». Пізніше в Агентстві з питань удосконалення діяльності Національної поліції (*National Police Improvement Agency* – NPIA) було заявлено, що модель «*використовує підхід до боротьби зі злочинністю і порушенням громадського порядку, керований аналітичною розвідкою і спрямований на вирішення проблем*» [13]. Ці джерела сходяться в тому, що основним компонентом моделі є «*розвідка*», причому NPIA і NCIS включають «*прийняття рішень*» і «*вирішення проблем*» у якості визначення завдань і подальшої взаємодії.

Водночас, право NIM називатися національною політикою не може бути остаточним, оскільки Хілл [14] стверджує, що «*проблеми у визначенні, пов'язані з поняттям політики, свідчать про те, що важко розглядати її як дуже специфічне і конкретне явище*». Однак, у моделі під «політикою» розуміють «*сукупність взаємопов'язаних рішень ... щодо вибору цілей і засобів їх досягнення в конкретній ситуації ...*» [15], що дає підстави сприймати NIM як «*політику*», яка стосується «*прийняття рішень на основі аналітичної розвідки*» із застосуванням «*обґрунтованих рішень*», тобто аналітичних продуктів [16]. Вибір «*цілей*» реалізується в різних формах, зокрема силові заходи, зниження рівня злочинності та порушень громадського порядку [13], а також досягнення «*стратегічних цілей*» [17]. Крім того, у 2000 році NIM став політикою Асоціації керівників поліції (*Association of Chief Police Officers*, ACPO) [18], що забезпечує широку поліцейську перспективу. А з прийняттям у 2002 році Закону про реформування поліції і обов'язковість упровадження NIM на національному рівні поліцейськими службами, перетворили цю «*політику поліції (ACPO)*» на «національну політику» [15].

Розроблена Національною службою кримінальної розвідки (NCIS) National Intelligence Model (NIM) була ребрендована і активно спонсорована Асоціацією керівників поліції (ACPO) та рекомендована міністру внутрішніх справ Джеку Строу у вересні 2000 року. Попри те, що NIM є певним чином продовженням Кентської моделі, все ж вони відрізнялися тим, що NIM визначала «*значно ширші масштаби і амбіції*» [19, с. 124]. Як зазначають Емей та ін. [20, с. 33], у своїй початковій формі Кентська модель, зосереджуючись лише на чотирьох видах злочинів (пограбування, автозлочини, квартирні крадіжки та наркотики), не мала на меті вплинути на загальну злочинність. На відміну від Кентської моделі, NIM включає вимогу щодо «стратегічної оцінки». Джон і Магуайр [21, с. 212] описують її як «*засновану на аналізі проблем ... і пріоритетів, встановлених ... внутрішніми і зовнішніми органами*».

Крім того, під час зародження NIM в Національній службі кримінальної розвідки (NCIS) та Міністерстві внутрішніх справ (Home Office) існував потенціал для перенесення політики з альтернативних поліцейських ініціатив, зокрема і COMPSTAT, Community Policing, нового публічного менеджменту (New Public Management - NPM) тощо. Наразі модифікація Кентської моделі була досить очевидною і, можливо, надала Міністерству внутрішніх справ зручну і своєчасну можливість просунутися як у напрямі правоохоронної діяльності, керованої аналітичною розвідкою, так і щодо посилення підзвітності. Джеймс [18, с. 132] зазначає, що NIM була привабливою пропозицією для Міністерства внутрішніх справ, оскільки це була «*раціональна модель, яка пропонувала певний рівень підзвітності*».

NIM & COMPSTAT

Потенційно сильною та конкурентною «*моделлю, керованою аналітичною розвідкою*», що представляла актуальний інтерес для поліції наприкінці минулого сторіччя, була американська модель «COMPSTAT», розроблена Джеком Мейплом у 1994 році під егідою Браттона [22], а згодом впроваджена в поліції Нью-Йорка. І NIM, і COMPSTAT спільно описуються як «*моделі аналітичної розвідки, що дозволяють здійснювати стратегічне управління і своєчасне спрямування ресурсів на боротьбу зі злочинністю*» [23]. COMPSTAT отримав значний суспільний інтерес і підтримку у Великій Британії завдяки схвальним повідомленням у ЗМІ про його впровадження та подальше зниження рівня злочинності у зв'язку з ініціативою «*нульової толерантності*» поліції Нью-Йорка [24]. У поліції Великої Британії низка відомих керівників поліції виявили кваліфіковану зацікавленість у впровадженні COMPSTAT [25; 26], але підтримка не була одностайною.

Браттон, комісар поліції Нью-Йорка, стверджував [27], що для того, щоб елемент COMPSTAT був успішним, він вимагав внутрішньої підзвітності, коли керівники дільниць відвідували щотижневі організаційні наради з контролю за злочинністю, щоб звітувати про результати своєї роботи. Ці наради, відомі в народі як «*кровопускання*», проводилися в «*насиченому даними середовищі*» [28] і були схожі на механізм і процеси постановки завдань і координації NIM. Процес COMPSTAT базувався на принципі «*нульової толерантності*» і приніс значні результати, а саме: різке, підтверджене незалежними експертами, зниження рівня зареєстрованої злочинності. Однак дотримання вимог і «*виконання*» безжально нав'язувалося і контролювалося Браттоном, який протягом 18-місячного періоду випробовування і впровадження програми перепризначив понад 30% керівників дільниць і звільнив чотирьох з п'яти своїх топкерівників [29, с. 136].

Певним чином COMPSTAT вплинув на розробку NIM, хоча б через додавання «*стратегічного елементу*», чого не було в Кентській моделі. Однак потреба в упровадженні стратегічного елементу вже проявлялась у попередніх проектах і зрештою увійшли до NIM [29, с. 33].

Започатковуючи NIM у Міністерстві внутрішніх справ Великої Британії, мала місце певна невизначеність щодо того, за яким саме напрямом діяльності закріпити модель. Спочатку, для розгляду і розробки, її було передано до Портфоліо щодо організованої злочинності, а потім переведено до Директорату зі зниження рівня злочинності (Crime Reduction Directorate). Після обговорення з ACPO NIM передали (навесні 2002 року) до Підрозділу з питань поліцейської політики (Policing Policy Unit) [30, с. 132]. Як уже зазначалося, Ретклiфф [31, с. 273] тісно пов'язує NIM з поліцейською діяльністю, керованою аналітичною розвідкою, стверджуючи, що «...майже неможливо обговорювати концепцію поліцейської діяльності, керованої аналітичною розвідкою, не посилаючись на NIM». Він продовжує цю думку, стверджуючи, що ILP і NIM «*...філософськи найбільш близькі до проблемно-орієнтованої поліцейської діяльності і, до певної міри, до механізму підзвітності CompStat*».

NIM & COMMUNITY POLICING

Community Policing не є новою концепцією, і в деяких аспектах вона має більш давнє походження, ніж її сучасні конкуренти. Емслі [32, с. 235] вважає, що хоча концепція Community Policing була сформульована наприкінці XX сторіччя, вона набагато давніша, «*ідеї та практики, які об'єднані в рамках цієї концепції, пройшли через всю історію поліції*». До кінця 1970-х років концепція Community Policing відроджувалася як робоча концепція серед керівників поліції [33, с. 9] і була охарактеризована як «*нова ортодоксія*» [34, с. 3]. Цей термін фігурує під низкою альтернативних назв, таких як «*сусідська поліція*», «*партнерство з громадою*» та «*залучення громади*» [35, с. 9], що може бути частково пов'язано з відсутністю його чіткого визначення, або ж із зручністю використання.

Незважаючи на тривалу історію Community Policing, чіткого, узгодженого серед фахівців, визначення не розроблено: за словами Фрідмана [36] в 1992 році, в літературі не було жодного визначення. Тіллі [10, с. 315] стверджує, що після всебічного огляду «*Community Policing широко схвалюється, але в той*

же час вважається, що вона майже не має сенсу». Роу [37, с. 72] припустив, що його визначення може «*здаватися розпливчастим і більш ніж амбітним*», а для сучасної поліції найбільш близькими до визначення є два набори з десяти принципів, перший з яких був запропонований Олдерсоном, а другий - Трояновичем і Буккеро [38]. Фрідман [36, с. 4] описав їх так «*Десять принципів Олдерсона стосуються роботи поліції в умовах свободи з акцентом на гарантуванні особистої свободи і вільного пересування, тоді як принципи, запропоновані Трояновичем і Буккеро, мають більше спільного з реалізацією концепції в конкретному поліцейському підрозділі*». Тому достатньо обґрунтованим є визначення **Community Policing**, сформульоване Фрідманом [36, с. 115], як

> *«політика і стратегія, спрямовані на досягнення більш ефективного і дієвого контролю над злочинністю, зниження страху перед злочинністю, поліпшення якості життя, підвищення якості поліцейських послуг і легітимності поліції шляхом активного використання ресурсів громади, спрямованого на зміну умов, що сприяють злочинності».*

Невизначене і потенційно неоднозначне значення цього терміну не завадило йому продовжувати широко використовуватися, хоча його широке застосування, можливо, сприяло його девальвації, і на думку деяких авторів, зробило цей термін майже беззмістовним [39, с. 211; 40, с. 104; 41, с. 376-377]. Однак ця думка не є однозначною, і Вільямсон [42, с. 153] описує концепцію Community Policing як «*бажаний стиль роботи поліції*», а Броган і Ніджхар [43, с. 1]. стверджують, що вона залишається «*популярним словом в англо-американській поліцейській практиці протягом останніх двох десятиліть*». Крім того, Community Policing продовжує залишатися предметом поточного огляду практиків [35; 44] і популярною темою серед сучасних дослідників і авторів, які пишуть про поліцейську практику [45; 46].

Наразі, саме рівень популярності та обізнаності, якого набула концепція Community Policing під час переходу від Кентської поліцейської моделі до NIM, дає змогу визнавати її як «*фактор впливу*» через перенесення політики [15, с. 60]. Виявлені відмінності між NIM і Кентською моделлю дозволяють припустити, що автори NCIS, можливо, під впливом ACPO, переглянули і модифікували модель Community Policing.

ILP і Кентська модель були виключно прерогативою поліції і самі по собі не вказували на модель широкого прийняття і застосування поза межами правоохоронних органів. Ні ILP, ні Кентська модель не виключають «*спільної роботи*» або партнерства, але їхній профіль, процеси і продукти потенційно більш обмежені і призначені для задоволення потреб поліцейської діяльності. Community Policing вимагає більш широкого залучення [36], ніж Кентська модель, поширюючись на соціальні ініціативи, такі як «*Сусідський патруль*» (Neighbourhood Watch) [15, с. 60], і, в умовах постійного прагнення до розслідувань і прийняття рішень на основі аналітичної розвідки, вимагає більш широкого доступу до даних та інформації. Це опосередковано вимагає співпраці з суспільством, громадськими організаціями та комерційними структурами, щоб забезпечити «*більш ефективний і дієвий контроль над злочинністю ... через активне використання ресурсів громади*» [36, с. 115].

Визнання того, що поліція не може ізольовано вирішувати проблеми зростання злочинності та порушень громадського порядку, було чітко визнано у Законі про боротьбу зі злочинністю та порушенням громадського порядку 1998 року (*The Crime and Disorder Act, CDA*) [15, с. 61]. Цей закон встановив «*партнерство за законом*» між поліцією та цивільними органами влади. Обов'язкове партнерство охоплювало 376 місцевих органів влади та сприяло створенню Партнерств зі зниження рівня злочинності та порушень громадського порядку (*Crime and Disorder Reduction Partnerships, CDRP*) і може розглядатися як «*фаза 1*» більшого залучення громадськості та співпраці. Таке партнерство передбачає обов'язковість проведення та опублікування аудиту злочинності та порушень громадського порядку, стратегії та цілей; обов'язковими є консультації з місцевою громадою. Відповідно Закон (CDA) надав нові повноваження місцевим органам влади та поліції, а також визначив вимогу розвивати міжвідомчі та громадські стратегічні партнерства для зниження рівня злочинності та порушень громадського порядку у своїй місцевості з опосередкованим очікуванням, що NIM буде підтримувати цю спільну роботу.

Однак це не вимагало обов'язковості взаємодії щодо розслідувань з більш широкою спільнотою в інших державних службах та структурах. Саме тому було включено наступне твердження до Кодексу правил NIM:

> *«NIM не обмежується використанням спеціалістами. Вона має відношення до всіх сфер правоохоронної діяльності: злочинності та її розслідування, порушень громадського порядку і громадської безпеки» [47, п. 3.1.3].*

Цей етап розглядається як «*фаза 2*» урядової ініціативи, спрямованої на підвищення узгодженості процесу розслідування, заснованого на аналітичній розвідці, у національному слідчому співтоваристві і, таким чином, сприяння більш тісному співробітництву [15, с. 61]. Наразі, це не було остаточним висновком, команда розробників NCIS, яка визначала NIM, була знайома з практикою Community Policing, хоча вони працювали в службі, яка зосереджувалася на боротьбі з тяжкими злочинами та організованою злочинністю. Кентська поліцейська модель була розроблена і впроваджена для використання на рівні округу і мала чітко виражену поліцейську специфіку. Не можна стверджувати, що вона була позбавлена міркувань Community Policing, але все ж таки, цей елемент був посилений при розробці NIM, таким чином, враховуючи популярність ідеї посилення партнерства [48]. У порівнянні з Кентською моделлю, NIM мав на меті привернути увагу більш широкої громадськості, мати більш широке застосування і відповідати вимогам, що вимагало безпосередньої взаємодії як із суспільством, так і з широкою правоохоронною спільнотою. У зв'язку з цим «Настанова» [49] була складена з великою кількістю посилань на «громадськість»: *«спільний підхід до охорони правопорядку»*, *«вимога участі інших установ та органів»*, співпраця, залучення, інформування та партнерство тощо[15, с. 62].

НОВИЙ ПУБЛІЧНИЙ МЕНЕДЖМЕНТ

Леві [50, с. 234] стверджував, що культура ефективності була «*домінуючою парадигмою в публічній адміністрації протягом щонайменше 20 років*», а тому це мало потенційний вплив на архітекторів і розробників NIM. До того ж, ключові розробники NIM (ACPO) знали, що для отримання схвалення Міністерством внутрішніх справ і прийняття на національному рівні, компонент «*управління ефективністю*» є привабливим стимулом. Співвідношення ціни і якості, управління за цілями і пріоритетне використання ресурсів – все це було характерним для «Ініціативи фіскального менеджменту» (*Fiscal Management Initiative* – FMI) консервативного уряду, яка еволюціонувала в Новий публічний менеджмент, що мало на меті сприяти кращому управлінню фінансами і ресурсами, шляхом впровадження комерційних практик у державну службу. Севедж [51, с.212] стверджує, що культуру діяльності, нав'язану поліції у відповідь на FMI та Новий публічний менеджмент, можна умовно поділити на три етапи: економія та результативність (1980-ті роки); ефективність (1990-ті роки); результати та виконання.

На етапі «економія та результативність» поліція була швидко включена в систему «цільових» державних органів Циркуляром Міністерства внутрішніх справ № 114 (1983), який заохочував застосування Нового публічного менеджменту [52]. Хоча Циркуляр МВС (114/1983) не був обов'язковим до виконання, його швидко прийняли як «*основоположний документ, що вплинув на думки і дії керівників поліції*» [53, с. 23]. Певним чином було простимульовано поліцейську діяльність із врахуванням трьох цілей (три Е) – результативність (efficiency), ефективність (effectiveness) та економічність (economy) про що Брукс [54, с. 1] зазначив «*розуміння того що виміряно, буде зроблено*».

Однак дослідження Везеріта [55] виявило, що на практиці цілі «*часто формулювалися на основі поганої, нерелевантної або неповної інформації*», що свідчило про те, що FMI/Новий публічний менеджмент у вигляді Циркуляру 114/83 не став стимулом для підвищення результативності та підзвітності. Навпаки, воно мало тенденцію до заохочення традиційних методів, діючи радше як гальмо, відвертаючи енергію і ресурси від впровадження прогресивних і потенційно більш ефективних ініціатив. Чого не вистачало Циркуляру 114/83 у 1980-х роках, так це структури: він не був модульованим, директивним і не супроводжувався стандартами, як у випадку з NIM, він не «*реалізовував фундаментальні принципи*» [15, с. 63] і дозволяв застосовувати їх на власний розсуд. Результатом стало різноманіття поліцейських практик, і Лейшман та ін. [15, с. 63] стверджували, що поліція була майже унікальною в державному секторі у своєму опорі Новому публічному менеджменту. Наприкінці 1980-х років цей опір збігся з «*узгодженим прагненням центрального уряду ... запровадити заходи з підвищення ефективності та посилення фінансової підзвітності в державному секторі з метою забезпечення ефективного використання коштів*» [56, с.178].

На наступному етапі «Ефективність», що асоціювався з поняттями аудит та інспектування, поліція вдосконалювала та застосовувала більш проактивні методи боротьби зі злочинністю, в деяких випадках стимульовані звітом Національної ревізійної комісії (National Audit Commission) [57] «*Допомога у розслідуванні – ефективна боротьба зі злочинністю*». Зрештою, це призвело до низки експериментів та ініціатив, включаючи поліцейську діяльність, керовану аналітичною розвідкою, як у Кентській поліцейській моделі [58, с. 210], хоча Севідж [51] припускає, що повна поява ILP збіглася зі створенням NIM. Іннес і Шептицький [59, с. 22] припускають, що відхід від традиційних методів мотивувався зростаючими вимогами до поліції бути більш підзвітною і «*економічно ефективною*», «*... нові практики ILP (і NIM) сприяли цим змінам*». Однак, стандартизація та узгодженість між силовими структурами разом з підвищенням «ефективності та підзвітності» все ще виявилися недосяжними

для Міністерства внутрішніх справ і Національної служби кримінальної розвідки (НМІС) [60, с. 34-35]. Скотт [61, с. 270] стверджував, що саме поширення культури результативності може змусити поліцію відволіктися від «*сфер, які важко піддаються кількісній оцінці*», таких як охорона громадського порядку та запобігання злочинності, і просто зосередитися на тому, яким чином їх оцінюють. Вимірювання відбувалося у двох формах: централізовано встановлені цілі та інспекційний режим. Інспекції НМІС були відносно неформальними, «*мало переймалися ретельністю тестування*»; це мало змінитися з приходом Нового публічного менеджменту, що фактично перетворило процес інспектування з «*ритуалу на примус до виконання*» [51, с. 96). На додаток до цього, НМІС збільшив свою владу і вплив кількома способами, по-перше, проводячи тематичні інспекції з поглибленим аналізом, а також щорічні інспекції [62]. По-друге, оприлюднюючи всі свої звіти - ефективно забезпечуючи, щоб непокірних було «*названо і присоромлено*», а також поширюючи передовий досвід; і, нарешті, поповнюючи свої ряди кваліфікованим персоналом, включаючи цивільних експертів у сфері фінансів та людських ресурсів. За допомогою цих інспекцій та наступних звітів поліцію заохочували переглянути й визначити процеси та процедури, які б відповідали цілям охорони правопорядку.

На наступному етапі нормами законів (Закон про поліцію та магістратські суди (Police & Magistrates Court Act - PMCA) 1994 року та Закон про регулювання слідчих повноважень (Regulation of Investigatory Powers Act) 2000 року) [15, с. 65-66] було запроваджено елементи управління ефективністю діяльності поліції, а також посилено контроль з боку центрального уряду через. PMCA фактично наділив Міністра внутрішніх справ повноваженнями запроваджувати обов'язкові щорічні цілі та показники ефективності (таргетування) діяльності поліції. У відповідь на це органи поліції були зобов'язані складати і публікувати щорічні плани роботи поліції, які, по суті, забезпечували підзвітність керівників поліції [63; 64]. Спочатку Джонс, Ньюберн і Сміт [15, с. 65] стверджували, що юридичні вимоги, встановлені PMCA, мали лише поверхневий і непрямий вплив на поліцію Великої Британії, стверджуючи, що модель належної процедури була «*безнадійно неадекватною*» і що переглянуті правила «*часто ігнорувалися і навіть могли бути контрпродуктивними*» [15, с. 65]. І навпаки, Ньюберн [65, с. 9] припустив, що PMCA ознаменував «*нову еру в роботі поліції з акцентом на боротьбу зі злочинністю*», таким чином, фактично заклавши основу для законодавчого прийняття NIM в більш широкому контексті поліцейської діяльності. Пізніше Райнер [15, с. 65] захистив PMCA як перший крок у забезпеченні підзвітності поліції та одну з найуспішніших практик, мотивованих Новим публічним менеджментом. Рівень значущих і довготривалих змін в ефективності роботи поліції та безпосередній вплив PMCA на правоохоронну практику і культуру залишаються дискусійними. Причину певної інертності в поліції, про яку повідомляють Джонс та ін. [15, с. 65], принаймні в централізованих підрозділах, та яку виявив Скоган [15, с. 65], який, посилаючись на свої дослідження в поліції США, припустив, що офіцери (особливо в елітних підрозділах) здатні чинити опір більшості змін, які намагаються запровадити за допомогою «стратегій уникнення».

NIM ЯК БІЗНЕС-МОДЕЛЬ

За словами Алана Бака, голови Консультативного комітету з питань боротьби зі злочинністю Асоціації суперінтендантів (Association Crime Advisory Committee), NIM спочатку призначався виключно для розвідувальних цілей [66]. Однак ця думка є помилковою, оскільки Міністерство внутрішніх справ, очевидно, було переконане, що NIM може працювати як бізнес-модель. Як зазначалося раніше, ця модель могла мати додаткову привабливість, надаючи можливість розширити культуру роботи в поліції, підтримуючи процес прийняття рішень на основі Кентської моделі прийняття рішень до рівня бізнес-моделі. Міністерство внутрішніх справ, вбачало додаткові переваги в тому, щоб нав'язати поліції таку бізнес-модель, про що свідчить наступна заява:

> *Важливо зазначити, що NIM стосується НЕ лише злочинності і НЕ лише розвідки – це модель, яка може бути використана для більшості сфер поліцейської діяльності .... NIM – це насамперед бізнес-модель для використання при розподілі ресурсів [67].*

Крім того, у Настанові по NIM («Guidance on the National Intelligence Model») (49, с. 9) ACPO підтримала таке більш широке застосування NIM, ніж як інструменту процесу ILP, зазначивши, що

> *«NIM - це бізнес-модель для правоохоронних органів» і «NIM є основною бізнес-моделлю для забезпечення правопорядку ...».*

Крім того, у посібнику зазначено:

> *«NIM схожа на будь-яку іншу бізнес-модель тим, що вона вимагає, щоб продукти мали практичне застосування» [49, с. 59].*

Навіть сучасні автори підтримують думку про те, що NIM по суті є бізнес-моделлю [15, с. 69]; в той час як Ретклiфф [31, с. 273] стверджує:

> *«Хоча NIM не є повним синонімом поліцейської діяльності, керованої аналітичною розвідкою, вона була прийнята як бізнес-модель».*

NIM ТА ЗНИЖЕННЯ РІВНЯ ЗЛОЧИННОСТІ

NIM, як законодавча вимога до поліції в Англії та Уельсі, має на меті підвищити результативність та ефективність розслідувань і знизити рівень злочинності [49]. Вона має більш широкі цілі, оскільки спрямована на підвищення рівня громадської безпеки, запобігання правопорушенням та злочинності [68], але це може бути вказівкою на її ключову функцію – зниження кримінальної активності за допомогою підходу, заснованого на аналітичній розвідці. Такий підхід має також підтримку, зазначаючи про наявність зв'язку між NIM та оперативною ефективністю, але такий підхід є дискусійним [69]. Однак він може забезпечити стандартизацію процесу за умови «дотримання» або відповідності мінімальним стандартам, що вимагає значних інвестицій і для більшості публічних послуг, і для ефективних змін у політиці та процесі правоохоронної діяльності. Тобто ключовою вимогою щодо реалізації аналітичної розвідки в правоохоронній діяльності є дотримання та схвалення NIM [70].

Іншим критично важливим фактором є своєчасна і пропорційна реакція на рішення, а це вимагає адекватної «*спроможності тактичного розгортання*» або просто «*адекватних ресурсів*». Зокрема, Урядовий офіс [71] заявляє, що

> *«NIM забезпечує проведення заходів, спрямованих на зниження рівня злочинності, порушень громадського порядку, антисоціальної поведінки та зловживання наркотичними речовинами» -*

це може бути бажаною метою, але жодних доказів на підтримку цього твердження не надано [15]. Як ILP та проблемно-орієнтованої поліцейська діяльність [72], NIM спочатку була сформульована як правоохоронна стратегія, спрямована на зниження рівня злочинності [31]. Спеціальний комітет у справах Уельсу (Select Committee on Welsh Affairs) [73] заявив, що NIM «*означає, що тепер ми можемо створювати стратегії, які знизять рівень злочинності і поліпшать якість життя в нашій громаді*». Однак залишається дискусійним питання, чи дійсно єдина «модель», запроваджена з метою підвищення результативності розслідувань і прийняття рішень щодо визначення завдань, покращує «якість життя». Як соціологи, так і кримінологи значною мірою підтримують думку про те, що причини та рівень злочинності залежать від широкого спектру факторів, які включають культурні, системні, економічні, освітні та правові чинники.

ОРГАНІЗАЦІЙНІ ЗМІНИ

Упровадження NIM спровокувало значні зміни в управлінні ресурсами в поліції [15]. Для впровадження моделі знадобилися додаткові «активи», а саме: знання, система, джерела та ресурси, а також вимоги щодо дотримання мінімальних стандартів, що прискорило перегляд та адаптацію процедур. Вона повинна була мати широкий вплив на процес прийняття рішень, формуючи напрям і визначаючи розподіл ресурсів. Орієнтуючись на розвиток аналітичної розвідки, NIM не була цілковитим нововведенням, а скоріше продовженням ILP, і, як зазначають Вуд і Ширінг [74, с. 55], «*поліцейська діяльність, керована аналітичною розвідкою [NIM] не стільки переосмислює роль поліції, скільки уявляє, як поліція може бути розумнішою*». В ідеалі, «*розумніша*» поліція повинна стати більш продуктивною і ефективною, що повинно призвести до зниження рівня злочинності і підвищення рівня безпеки в суспільстві. Дійсно, потужність «*сили змін*» визначається її «*впливом на ділову активність організації; потужна сила змін може призвести або до значного зниження, або до підвищення результативності*» [75, с. 538].

Осборн і Браун [76, с. 184] припускають, що існує чотири основні стимули для інновацій та змін у державній службі, які можна класифікувати наступним чином: «*дослідження*», «*ринковий попит*», «*політичний імператив*» і «*потреба бути поміченими в роботі*». Потенційно всі ці фактори вплинули на рішення щодо просування NIM як робочого синтезу ILP і проблемно-орієнтованої поліцейської діяльності. Наприкінці тисячоліття в засобах масової інформації продовжував існувати попит (що переносився в суспільну свідомість і, отже, був «ринковим»), а нова лейбористська ініціатива забезпечила політичний імператив для сприяння підвищенню результативності роботи поліції [15]. Зрештою, було прийнято цю модель, незважаючи на критику з боку деяких кіл, включаючи скаргу на те, що модель була «*надмірно складною, занадто важкою*» [18, с. 126]. Впровадження NIM спричинило «*бурхливу діяльність*», що призвело до реорганізації підрозділів, набору аналітичного персоналу

і регулярності проведення зборів (постановка завдань і координація), а також спричинило появу великої кількості документації [15].

Таким чином, з появою у Великій Британії Закону про реформування поліції 2002 року та включенням до Національного плану розвитку поліції на 2003-2006 роки, прийняття NIM стало обов'язковим для всіх 43 поліцейських осередків Англії та Уельсу до квітня 2004 року. NIM була широко сприйнята як ефективний синтез, що поєднує заходи безпеки та розслідування правопорушень з аналітичною розвідкою, тобто, в основі якого лежить використання аналітичної розвідки для впливу на прийняття стратегічних і тактичних рішень, а також на розподіл ресурсів. Як бізнес-модель або процес, заснований на аналітичній розвідці, дотримання NIM має на меті забезпечити низку переваг для користувача, серед яких безпеку громади, зниження рівня злочинності та контроль над злочинністю і порушенням громадського порядку. Критично важливим є те, що використання NIM не обмежене лише поліцейською діяльністю. Низка державних служб і не лише правоохоронні органи перейшли на цю модель у 2004-2005 роках. Дійсно модель є достатньо складною, а критерії відповідності, що містяться у відповідних нормах та мінімальних стандартах, є досить вимогливими для тих, хто приймає цю модель, для досягнення стандартизованого процесу розслідування і прийняття рішень на основі аналітичної розвідки.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Кардашевський Ю.Р. Становлення моделі правоохоронної діяльності, керованої аналітичною розвідкою. *Наука і правоохоронна*. 2023. №1. С.117-125.
2. Smith, Angus (1997). *Intelligence Led Policing*. Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts.
3. *Global Justice Information Sharing Initiative. National Criminal Intelligence Sharing Plan* (2003). Washington, DC: U.S. Department of Justice.
4. Ratcliffe, J.H. (2016). *Intelligence-Led Policing*. 2nd edn. New York: Routledge.
5. Carter, J.G. (2016). Institutional pressures and isomorphism: the impact on intelligence-led policing adoption. *Police Quarterly*, 19(4), 435–460.
6. Carter, D.L. (2009). *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*. 2nd edn. Washington, DC: Office of Community Oriented Policing Services, U.S. Department of Justice.
7. Carter, J.G. (2013). *Intelligence-Led Policing: A Policing Innovation*. El Paso, TX: LFB Scholarly Publishing.
8. Anderson, Richard (1997). *Intelligence-Led Policing: A British Perspective*. Angus Smith, editor. Lawrenceville, NJ: IALEIA.
9. Maguire, M. (2008). Criminal investigation and crime control. In T.Newburn (ed.) *Handbook of Policing*. Cullompton: Willan Publishing, 430-464
10. Tilley, N. (2003). Community Policing, Problem Oriented Policing and Intelligence-Led Policing. In T. Newburn (Ed.) *Handbook of Policing*, Cullompton: Willan Publishing, 311-339.
11. Modafferi, Peter & Philip Lynn (1999). Local Law Enforcement and Intelligence Led Policing / Intelligence Models and Best Practices. Lawrenceville, NJ: International Association of Law Enforcement Intelligence analysts.
12. National Criminal Intelligence Service. (2000). *The National Intelligence Model*. London: NCIS Corporate Communications.
13. National Police Improvement Agency NPIA, (2007). *Practice Advice on Resources and the People Assets of the National Intelligence Model*. Retrieved from http://www.npia.police.uk/en/9015.html
14. Hill, M. (2009). *The Public Policy Process* (5th ed.). Harlow: Pearson Education.
15. Nick, Osborn (2012). *To what degree have the non-police public services adopted the National Intelligence Model*? University of Portsmouth.
16. John, T. & Maguire, M. (2004). *The National Intelligence Model: Key lessons from early research*. Home Office Online Report 30/04. London. Retrieved from http://library.npia.police.uk/docs/hordsolr/rdsolr3004.pdf
17. John, T. & Maguire, M. (2004). *The National Intelligence Model: Early Implementation Experience in Three Police Force Areas*. Cardiff University Working Paper Series 50. Cardiff: Cardiff University.
18. NPIA (2009). National Police Improvement Agency: National Intelligence Model. Retrieved from http://www.npia.police.uk/en/9015.html
19. James, A. (2011). *The Influence of Intelligence-led policing Models on investigative Policy and Practice in Mainstream Policing 1993-2007*: Division, Resistance and Investigative Orthodoxy. Unpublished PhD thesis: London School of Economics.
20. Amey, P., Hale, C. & Uglow, S. (1996). *Development and Evaluation of a Crime Management Model: Police Research Series Paper 18*. London: Home Office.

21. John, T. & Maguire, M. (2002). *The National Intelligence Model: key lessons from early research, Home Office Online Report 30/04*. London: HMSO. Retrieved from http;//www.homeoffice.gov.uk/pdfs04/rdsolr30004.pdf.
22. Dussault, R. (March 31, 1999). Jack Maple: Betting on Intelligence. *Government Technology*. Retrieved from http://www.govtech.com/magazines/gt/Jack-MapleBetting-on- Intelligence.html
23. Ministry of Justice – New Zealand (2005). *Research on the Effectiveness of Police Practice in Reducing Residential Burglary*; 6: Police Organisation.
24. Loveday, B. (2005). The challenge of police reform. *Public Money and Management*, 25, 275-280.
25. Hayes, B. (1998). Applying Bratton to Britain: the need for a sensible compromise. In M. Weatheritt (Ed.) *Zero Tolerance Policing: What does it mean and is it right for policing in Britain? London: Police Foundation*, 13-24.
26. Griffiths, W. (1997). *Zero Tolerance: Policing a Free Society (Choice in Welfare)*. London: IEA Health & Welfare Unit.
27. Bratton, W. (1998). *Turnaround: How America's Top Cop Reversed the Crime Epidemic*. New York: Random House.
28. Weisburd, D., Mastrofski, S., McNally, A. M. & Greenspan, R. (2001). *COMPSTAT and Organizational Change*. Washington DC: Police Foundation.
29. Maple, J. (1999). *The Crime Fighter: Putting the Bad Guys Out of Business*. New York: Doubleday.
30. Grieve, J. (2004). Developments in UK Criminal Intelligence. In J. Ratcliffe (Ed.) *Strategic Thinking in Criminal Intelligence* (2nd Ed.). Annandale: New South Wales Federation Press, 25-36.
31. Ratcliffe, J.H. (2008). Intelligence-led policing. In Wortley, R., Mazerolle, L. and Rombouts, S. (Eds.) *Environmental Criminology and Crime Analysis*. Cullompton, Devon: Willan Publishing, 263-282.
32. Emsley, C. (2007). Community Policing/Policing and Communities: Some Historical Perspectives. *Policing*, 1 (2), 235-243.
33. Mackenzie, S. & Henry, A. (2009). *Community Policing: a Review of the Evidence*. Scottish Government Social Research Paper. Retrieved from http://www.scotland.gov.uk/Resource/Doc/292465/0090209.pdf
34. Eck, J.E. & Rosenbaum, D.R. (1994). The New Police Order: Effectiveness, Equity and Efficiency in Community Policing. In D.R. Rosenbaum (ed.), *The Challenge of Community Policing: Testing the Promises*. London: Sage.
35. Rix, A., Joshua, F., Maguire, M & Morton, S. (2009). *Improving public confidence in the police: a review of the evidence: Home Office Research Report 28*.
36. Friedmann, R.R. (1996). Community Policing: Some Conceptual and Practical Considerations. *Home Affairs Review*, XXXIV (6), 114-23.
37. Rowe, M. (2008). *Introduction to Policing*. London: Sage.
38. Trojanowicz, R. and Bucqueroux, B. (1990). *Community Policing: A Contemporary Perspective*. Cincinnati: Anderson Publishers
39. Manning, P.K. (1984). Community Policing. *American Journal of Police*, 3(2), 205-27.
40. Bayley, D.H. (1994). *Police for the Future*. Oxford: Oxford University Press.
41. Tilley, N. (2008). Intelligence-led Policing. In T. Newburn & P. Neyroud (Eds.), *Dictionary of Policing*. Cullompton: Willan Publishing, 146-8.
42. Williamson, T. (2005). Editorial - Community Policing. *Journal of Community and Applied Social Psychology*, 15, 153-5.
43. Brogan, M & Nijhar, P. (2005). *Community Policing: International Concepts*. Cullompton: Willan.
44. Mason, M. (2009) *Findings from the second year of the national Neighbourhood Policing Programme evaluation*. Home Office Research Report 14. London: Home Office.
45. Innes, M., Abbott, L., Lowe, T. & Roberts, C. (2009). Seeing Like a Citizen: Field Experiments in Community Intelligence-Led Policing. *Police Practice and Research*, 10(2), 99-114.
46. Peak K.W. & Glensor, R.W. (2011). *Community Policing and Problem Solving: Strategies and Practices*. London: Prentice Hall.
47. Home Office (2002). *The National Policing Plan 2003/2006*. London: HMSO.
48. The Scottish Government. (2010). *Community Policing: a Review of the Evidence*. Retrieved from http://www.scotland.gov.uk/Publications/2009/11/19091609/3
49. ACPO (2005). *Practice Advice on Core Investigative Doctrine*. Cambourne: National Centre for Policing.
50. Levy, R. (2010, May). New Public Management: End of an Era. *Public Policy and Administration*, 25 (2), 234-240.
51. Savage, S. (2007). *Police Reform: Forces for Change*. Oxford: Open University Press.
52. Burrows, J. & Lewis, H. (1998). *Directing Patrolling: a study of uniformed policing*. London: Home Office Research & Planning Unit.
53. ACPO (2008). *Submission of the Police Reform Green Paper: The Future of Policing.* London: ACPO.
54. Brooks, S. (2010*). What gets measured gets done*. Retrieved from http://www.guardianpublic.co.uk/police-targets-crime-brooks-comment
55. Holdaway, S. (1989). Discovering Structure: Studies of the Police Occupational Culture. In M. Weatheritt (Ed.) *Police Research: Some Future Prospects*. London: Avebury.

56. Walsh, K. (1995). *Public Services and Market Mechanisms: Competition, Contracting and the New Public Management*. London: Macmillan.
57. National Audit Commission. (1993). *Helping with Enquiries – Tackling Crime Effectively*. London: HMSO.
58. John, T. & Maguire, M. (2007). Criminal Intelligence and the National Intelligence Model. In T. Newburn, T. Williamson & A. Wright (Eds.), *Handbook of Criminal Investigation*. Cullompton: Willan Publishing, 199-225.
59. Innes, M. & Sheptycki, J. (2004). From detection to disruption: intelligence and changing logic of police crime control in the United Kingdom. *International Criminal Justice Review*, 24, 1-24.
60. HMIC (1997). *Policing with Intelligence: Criminal Intelligence*. Retrieved from http://www.nationalarchives.gov.uk/EORecords/HO/421/2/hmic/pintell.htm
61. Scott, J. (1998). Performance culture: the return of reactive policing. *Policing and Society*, 8, 269–288.
62. Reiner, R. (2000). *The Politics of the Police*, (3rd ed.). Oxford: Oxford University Press.
63. Jones, T. & Newburn, T. (1997). *Policing after the Act: Police and Magistrates Court Act 1994*. London: Policy Studies Institute.
64. Jones, T. & Newburn, T. (2002). The transformation of policing: Understanding current trends in policing systems. *British Journal of Criminology*, 42, 129-146.
65. Newburn, T., Williamson, T & Wright, A. (Eds.) (2003*). Handbook of Policing. Cullompton*: Willan Publishing.
66. IntelligenceAnalysis.net (2009). *NIM and Intelligence*. Retrieved from http://www.intelligenceanalysis.net/index.htm.
67. Home Office (2008). *Home Office Statistical Bulletin, Crime in England and Wales 2007/08*. C. London: HMSO.
68. Grampian Police (2010). *National Intelligence Model*. Retrieved from http://www.grampian.police.uk?About.aspx?id=204&pid=30;31;227
69. Blair, I. (2003). *Report in Committee to the Metropolitan Police Authority*. Retrieved from http://www.mpa.gov.uk/committees/mpa/2003/030227/15/
70. NYPA: North Yorkshire Police Authority (2007). *Intelligence Strategy 2007-2012*. Retrieved from http://www.nypa.gov.uk/CHttpHandler.ashx?id=508&p=0
71. *Government Office of the North East* (2010). Retrieved from http://www.safeinteesvalley.org/dsc/index.html
72. Goldstein, H. (1990). *Problem-Oriented Policing*. New York: McGraw Hill. Retrieved from http://www.popcenter.org/library/reading/pdfs/goldstein_book.pdf
73. Select Committee on Welsh Affairs (2005). *Fourth Report*. Retrieved from http://www.publications.parliament.uk/pa/cm200405/cmselect/cmwelaf/46/4606.htm
74. Wood, J. & Shearer, C. (2007). *Imagining Security*. Cullompton, Willan Publishing.
75. Strebel, P. (1997). Mastering Change. In T. Dickson and G. Bickerstaff (Eds.), *Financial Times Mastering Management*. London: Pitman Publishing.
76. Osborn, S.P. & Brown, K. (2005). *Managing Change and Innovation in Public Service Organisations*. Abingdon, Oxford: Routledge.

DOI: https://doi.org/10.36486/978-966-2310-66-5-8

Для мене не важливо, на чиєму боці сила; важливо те, на чиєму боці право.

Віктор Гюго

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

Наталія Свиридюк
Ганна Форос

Дотримання прав людини має важливе значення як для короткострокової, так і для довгострокової ефективності поліцейської діяльності, включаючи ILP. Діяльність правоохоронних органів, яка не поважає та не захищає права людини, є контрпродуктивною у довгостроковій перспективі, оскільки вона підриває суспільну довіру до поліції, а також є неефективною. Наприклад, етнічне профілювання є дискримінаційним, і воно також виявилося неефективним, оскільки його можна легко обійти. Злочинні групи можуть уникнути розкриття шляхом вербування осіб, які не відповідають заздалегідь визначеним профілям. Альтернативні, законні методи профілювання, засновані на конкретних доказах злочинної поведінки та аналітиці, а не на дискримінаційних припущеннях, можуть бути використані як більш ефективний інструмент поліцейської діяльності.

Норми прав людини викладені в міжнародно-правових документах і стандартах, таких як обов'язкові договори, наприклад, Міжнародний пакт про громадянські та політичні права [1] і Конвенція Ради Європи про захист прав людини та основних свобод [2]. Для здійснення прав, закріплених у цих договорах, держави повинні створити правову та інституційну основу для реалізації прав людини на національному рівні. У цьому контексті, одним з основних обов'язків поліції є захист осіб від дій, які порушують їхні права людини, у тому числі внаслідок злочинів і тероризму та дотримання цих прав. У боротьбі та запобіганні злочинності поліція повинна діяти відповідно до національного законодавства та міжнародних стандартів. Будучи проактивною формою поліцейської діяльності, ILP також має міцно закріплятися на правозахисних нормах. ILP має підвищити рівень захисту прав і свобод людини та повинна здійснюватися таким чином, щоб повною мірою забезпечувати дотримання прав людини, що відповідає ключовим принципам демократичної поліцейської діяльності.

ЗАГАЛЬНІ ПРИНЦИПИ ПРАВ ЛЮДИНИ

З метою забезпечення відповідності діяльності ILP міжнародним стандартам у галузі прав людини та попередження негативного впливу на реалізацію прав людини, при розробці та впровадженні ILP на національному рівні необхідно дотримуватися низки основних принципів:

Правова, адміністративна та інституційна основа для реалізації ILP

ILP має ґрунтуватися на чітких і точних правових та адміністративних положеннях, що визначають умови її здійснення; мають бути надані адекватні гарантії, що це не порушує права людини. Національна модель ILP повинна включати закони та нормативні акти, які чітко та точно визначають повноваження, надані відповідним установам, та вимоги, які необхідно дотримуватись під час збору, обробки, аналізу та обміну різними типами даних, інформації та аналітичних продуктів. Усі національні закони, нормативні акти, політика та практика щодо ILP мають повністю відповідати міжнародним стандартам прав людини та зобов'язанням ОБСЄ. Крім того, співробітники правоохоронних органів, залучені до ILP, повинні отримати належну підготовку щодо застосування цих законів та правил відповідно до міжнародних стандартів у галузі прав людини.

Законність, необхідність і пропорційність обмежень прав людини

Хоча низка прав людини, таких як заборона катувань і певні елементи права на справедливий судовий розгляд справи, є абсолютними і не можуть бути обмежені за жодних обставин, міжнародні угоди з прав людини допускають запровадження обмежень на певні права, але лише в межах суворо

визначених параметрів. Права, які можуть бути обмежені, включають свободу пересування, право на особисту недоторканність, свободу думки, зібрань та об'єднань, а також свободу сповідувати свою релігію чи переконання [3]. Відповідно, обмеження, застосоване у зв'язку з ILP, є допустимим, лише якщо воно передбачено законом, необхідні у демократичному суспільстві в інтересах законної мети, конкретно зазначеної у відповідних міжнародних стандартах прав людини та пропорційно цій меті: тобто право є правилом, обмеження мають залишатися винятком, а втручання завжди повинні бути найменшими інтрузивними засобами досягнення мети.

Рівність і недискримінація

Відповідно до своїх міжнародних зобов'язань у сфері прав людини, держави-учасниці ОБСЄ зобов'язалися забезпечити права людини та основні свободи кожному, хто перебуває під їхньою юрисдикцією, без будь-якої різниці, як-от раси, кольору шкіри, статі, мови, релігії, політичних чи інших переконань, національного чи соціального походження, майнового стану, народження чи іншого статусу [4]. Захист рівності перед законом та заборона дискримінації є основними обов'язками поліції в демократичному суспільстві [5]. Збираючи, обробляючи та аналізуючи інформацію та розвідувальні дані, правоохоронні органи повинні, наприклад, утримуватися від дискримінаційного профілювання. Подібним чином, в частині прийняття рішень на основі аналітики даних, органи влади повинні приділяти належну увагу, щоб уникнути надмірного контролю над певними громадами, з метою недопущення надмірно жорстких заходів, що може призвести до дискримінації. Особливу увагу слід також приділити різному впливу стратегічних рішень у сфері поліцейської діяльності на жінок та чоловіків. Тому підхід, який враховує різноманіття та гендерні аспекти, має бути включений у всі заходи ILP, які слід регулярно перевіряти на предмет будь-якого дискримінаційного впливу, який вони можуть мати на жінок і чоловіків або на окремі спільноти.

Ефективні засоби правового захисту, нагляд і підзвітність

Міжнародні стандарти у галузі прав людини передбачають право кожної людини, якщо права або свободи порушуються, на ефективні засоби правового захисту та надання таких засобів правового захисту компетентним судовим, адміністративним або законодавчим органом [1]. Оскільки ILP може призвести до потенційно далекосяжних утручань у широкий спектр прав людини, важливими є ефективні та доступні засоби правового захисту у разі порушення прав людини внаслідок ILP. Крім того, для забезпечення підзвітності установ та окремих співробітників правоохоронних органів, залучених до ILP, необхідно запровадити надійні механізми внутрішнього та зовнішнього контролю. Такі механізми можуть включати контроль та нагляд за виконавчими органами, законодавчими наглядовими комітетами та незалежним зовнішнім наглядом і механізмами розгляду скарг, які надають особі можливість одержання захисту. Судовий контроль над такими діями, як, наприклад, таємний збір даних та їх аналіз, особливо важливий для забезпечення належних гарантій проти зловживань під час застосування ILP [3].

ПРАВО НА ОСОБИСТУ НЕДОТОРКАННІСТЬ

Збір даних та інформації, а також їх обробка, аналіз і обмін, які є невід'ємними елементами ILP, можуть мати серйозні наслідки для захисту прав людини, зокрема, але не тільки, для права на особисту недоторканність.

Стаття 17 «Міжнародного пакту про громадянські та політичні права» (ICCPR) [1] передбачає, що ніхто не може зазнавати свавільного або незаконного втручання в його особисте життя, сім'ю, недоторканність житла чи кореспонденції, і що кожен має право на захист закону від такого втручання [1]. Щоб втручання не було «свавільним» або «незаконним», необхідно дотримуватися зазначеного: втручання мають бути передбачені законом, який, у свою чергу, має відповідати положенням, цілям і завданням ICCPR; і вони повинні бути розумними за конкретних обставин [6]. Держави-учасниці ОБСЄ підтвердили право на захист приватного та сімейного життя, місця проживання, листування та електронних комунікацій, а також необхідність уникати неправомірного чи свавільного втручання держави у сферу особи [7].

Різні явні та приховані методи збору інформації представляють різний ступінь втручання в право на особисту недоторканність. До цих методів відносяться: використання спеціальних методів розслідування та інших таємних слідчих заходів, включаючи спостереження за приватними об'єктами або місцем проживання, перехоплення повідомлень, використання агентів під прикриттям та інформаторів, а також доступ до банківських рахунків та іншої конфіденційної інформації [3], а також права людини в умовах розслідування тероризму [8; 9; 10]. Ефективний контроль з боку судових чи

інших незалежних органів за допомогою попереднього дозволу, нагляду або перевірки постфактум є найважливішим для забезпечення законності таких заходів. Крім того, їх слід використовувати лише у серйозних випадках і відповідно до серйозності справи, яка розслідується [9; 10].

Значну увагу привертає питання наслідків для права на особисту недоторканність масового стеження за комунікаціями. Європейський суд з прав людини визнав відеоспостереження такими, що порушують право на особисту недоторканність, дозволяючи здійснювати моніторинг повідомлень і даних практично будь-якої людини в країні, навіть осіб, які не входять до початкових заходів, де розпорядження про такі заходи відбувається виключно у сфері виконавчої влади та без оцінки суворої необхідності [11; 12]. На відміну від адресного спостереження, яке зазвичай ґрунтується на попередній підозрі та за умови попереднього судового або виконавчого дозволу, програми масового спостереження не дозволяють окремо оцінювати пропорційність до застосування таких заходів у кожному випадку і, таким чином, підривають саму суть права на особисту недоторканність [13; 14].

Захист даних

Захист даних є важливою частиною права на приватне життя, що має особливе значення для ILP. Комітет Організації Об'єднаних Націй з прав людини, орган, якому доручено стежити за виконанням ICCPR, підкреслив, що збір і зберігання персональної інформації на комп'ютерах, банках даних та інших пристроях має регулюватися законом. Крім того, необхідно вжити ефективних заходів для забезпечення того, щоб інформація про приватне життя особи не потрапила до будь-кого, хто не уповноважений законом отримувати, обробляти та використовувати її [3]. Низка міжнародних та регіональних документів містить більш конкретні дані принципи захисту, які необхідно поважати з метою забезпечення повного дотримання права на особисту недоторканість.

Наприклад, Конвенція Ради Європи про захист осіб щодо автоматизованої обробки персональних даних вимагає від сторін Конвенції гарантувати, що персональні дані, які піддаються автоматизованій обробці [15]:

> *отримані та оброблені чесно й законно;*
>
> *зберігаються з визначеними та законними цілями і їхнє використання не є несумісним з цими цілями;*
>
> *адекватні, відповідні та не надмірні щодо цілей, для яких вони зберігаються;*
>
> *точні та, якщо необхідно, актуальні;*
>
> *зберігаються у формі, яка дозволяє ідентифікувати суб'єктів даних не більше, ніж це потрібно для цілей, для яких ці дані зберігаються.*

Крім того, Конвенція забороняє автоматичну обробку конфіденційних даних, як-от: дані, що розкривають расове походження, політичні погляди, релігійні чи інші переконання, а також дані про здоров'я, сексуальне життя або кримінальний досвід без відповідних гарантій у внутрішньому законодавстві [15]. Вона також передбачає гарантії та засоби правового захисту, які мають бути доступні особам, які є суб'єктами збережених даних [15].

Конвенція встановлює суворі обмеження та застереження щодо застосування положень, подібних до зазначених вище. Будь-які обмеження мають бути передбачені законом і бути необхідними в демократичному суспільстві в інтересах законної мети, проголошеної в Конвенції, наприклад, такої як державна безпека, громадська безпека або припинення злочину [15]. Поняття «необхідність», як це розуміється в міжнародних стандартах з прав людини, враховує пропорційність досягнутої мети.

Посібник ОБСЄ «Права людини в умовах розслідування тероризму» містить огляд передової міжнародної практики, заснованої на вищезазначених принципах та інших міжнародних стандартах у цій галузі [8]. З метою забезпечення дотримання міжнародних стандартів у галузі прав людини, вказані практики повинні бути орієнтиром для політиків та працівників правоохоронних органів при розробці та здійсненні ILP.

ІНШІ ПОТЕНЦІЙНІ РИЗИКИ ДЛЯ ПРАВ ЛЮДИНИ, ПОВ'ЯЗАНІ З ILP

Права на особисту недоторканність, включаючи захист даних, є важливими для здійснення широкого спектру інших прав і основних свобод, таких як: право на свободу переконань і на вільне їх виявлення; свободу шукати, одержувати та поширювати інформацію; свободу мирних зібрань та асоціацій; свободу світогляду та віросповідання, серед іншого. Але збір і використання інформації та розвідданих може також безпосередньо впливати на здійснення інших прав, таких як право на

справедливий суд, право на свободу та особисту недоторканність, а також заборона катувань та інших видів жорстокого поводження [3].

Наприклад, під час публічних акцій протесту використання стратегії управління натовпом, відомої як «утримання», з метою розвідувального пошуку шляхом примусу мирних маніфестантів і навіть випадкових перехожих розкривати свої імена та адреси при виході з «утримання», викликало критику за те, що це може перешкоджати здійсненню права на мирні збори [16]. Арешт на підставі реєстрації відповідної особи у базі даних правоохоронних органів, яка не забезпечує належного захисту від свавільного втручання у право на особисту недоторканність і не базується на іншій інформації, яка підтверджує наявність обґрунтованих підозр, що заарештована особа вчинила або збиралася вчинити конкретне правопорушення, суперечить праву на свободу та недоторканність [17].

Що стосується збору, обробки, аналізу та обміну інформацією, у тому числі в рамках ILP, особливе значення має той факт, що використання в судовому розгляді інформації, отриманої внаслідок тортур, є абсолютно забороненим міжнародним правом. Її використання як доказ в суді порушує права на належний і справедливий судовий розгляд. Забороняється збір, передача та отримання інформації навіть якщо вона не призначена для використання у судових провадженнях [18].

Ці занепокоєння особливо актуальні, коли обмінюються інформацією та аналітичними висновками. Використання інформації, отриманої із застосуванням тортур, з третьої країни, навіть якщо інформацію отримано лише для оперативних цілей, може зробити приймаючу державу співучасником вчинення міжнародно-протиправних дій [18].

> *Таким чином, під час реалізації ILP повинні бути вжиті відповідні гарантії для забезпечення того, щоб інформація та аналітичні висновки, отримані незаконним шляхом, незалежно від того, чи то в країні, чи за її межами, не використовувалися всупереч міжнародному та національному праву.*

ВИКОРИСТАНІ ДЖЕРЕЛА

1. United Nations General Assembly. International Covenant on Civil and Political Rights (ICCPR). No. 14668, United Nations Treaty Series, Vol. 999 (New York: 16 December 1966). Retrieved from www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx
2. Council of Europe. Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), (4 November 1950). Retrieved from www.echr.coe.int/pages/home.aspx?p=basictexts
3. OSCE. Guidebook Intelligence-Led Policing (2017). TNTD/SPMU Publication. Series Vol. 13. Vienna. Retrieved from https://www.osce.org/files/f/documents/d/3/327476.pdf
4. OSCE. Concluding Document of the Vienna Meeting 1986 of Representatives of the Participating States of the Conference on Security and Co-operation in Europe, held on the basis of the provisions of the Final Act relating to the follow-up to the Conference (Vienna: 1989). Retrieved from www.osce.org/mc/40881?download=true
5. OSCE. Guidebook on democratic policing, by the Senior Police Adviser to the OSCE Secretary General, 2nd Edition (Vienna: OSCE, 2008b). Retrieved from www.osce.org/spmu/23804
6. United Nations Human Rights Committee. CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (8 April 1988). Retrieved from https://www.refworld.org/docid/453883f922.html
7. OSCE. Document of the Moscow Meeting of the Conference on the Human Dimension of the CSCE (Moscow, 3 October 1991). Retrieved from www.osce.org/odihr/elections/14310
8. OSCE. Human rights in counter-terrorism investigations – A Practical Manual for Law Enforcement Officers. (Warsaw: Office for Democratic Institutions and Human Rights (ODIHR) and Transnational Threats Department (TNTD), 2013). Retrieved from www.osce.org/ odihr/108930?download=tru
9. OSCE. ODIHR/TNTD (2013: 33-46). On legal as well as technical aspects of electronic surveillance in particular.
10. UNODC. Current Practices in Electronic Surveillance in the Investigation of serious and organized crime (Vienna: United Nations Publication, 2009). Retrieved from www.unodc.org/documents/ organized-crime/Law-Enforcement/Electronic_surveillance.pdf
11. European Court of Human Rights. Case of Szabo and Vissy v. Hungary. Application No. 37138/14 (Strasbourg: 12 January 2016). Retrieved from www.statewatch.org/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY.pdf
12. European Court of Human Rights. Case of Roman Zakharov v. Russia. Application no. 47143/06 (Strasbourg: 4 December 2015). Retrieved from lovdata.no/static/EMDN/emd-2006-047143.pdf
13. United Nations General Assembly. Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson. Annual Report to the UN General Assembly, 23 September 2014, A/69/397.

14. United Nations General Assembly. Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. Report to the UN Human Rights Council, 21 February 2017, A/HRC/34/61.
15. Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series, No. 108 (Strasbourg: 28 January 1981). Retrieved from conventions.coe.int/Treaty/en/Treaties/Html/108.htm
16. United Nations General Assembly. Special Rapporteur on the rights to freedom of peaceful assembly and of association Maina Kiai, Addendum, Mission to the United Kingdom of Great Britain and Northern Ireland. Report to the UN Human Rights Council, 17 June 2013, A/HRC/23/39/Add.1. Retrieved from www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/ Session23/A-HRC-23-39-Add1_en.pdf
17. European Court of Human Rights. Case of Shimovolos v. Russia. Application No. 30194/09 (Strasbourg: 21 June 2011). Retrieved from hudoc.echr.coe.int/ eng#{“appno”:[“30194/09”],”itemid”:[“001-105217”]}
18. United Nations General Assembly. Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment, Juan E. Méndez. Report to the UN Human Rights Council, 10 April 2014, A/HRC/25/60. Retrieved from ap.ohchr.org/documents/dpage_e.aspx?m=103

ІНСТИТУЦІЙНА ХАРАКТЕРИСТИКА КРИМІНАЛЬНОГО АНАЛІЗУ

DOI: https://doi.org/10.36486/978-966-2310-66-5-9

Зусилля аналітика – це те, що створює інформацію, незалежно від того, «побудована» ця інформація чи «видобута».

International Association of Crime Analysts (IACA)

РОЗДІЛ 9
Зарубіжні особливості інституційного становлення кримінального аналізу

Владислав Бурангулов

Кримінальний аналіз як інституційне забезпечення правоохоронної чи безпекової діяльності є порівняно новим явищем. Наразі формалізовані процеси діяльності спеціалізованих підрозділів щодо аналізу та встановлення злочинів є вже сучасною історією. Водночас багато дослідників вказують на глибокий історичний ракурс кримінального аналізу, апелюючи певними аналогіями щодо змісту, логіки й послідовності процесів.

Зокрема, у виданні Масачусетської асоціації аналітиків злочинності (*Massachusetts Association of Crime Analysts (MACA)*) зазначається, що як концепція, у своїй основній формі, кримінальний аналіз має бути лише трохи молодшим за сам злочин. Перший злочин не потребував аналізу, оскільки він ще не був частиною шаблону чи тенденції. Другий міг бути пов'язаним з першим, а третій – або з першим, або з другим, або з обома. Кожний наступний злочин мав більше шансів бути пов'язаним з попереднім, і, ймовірно, згодом і сформувалася перша модель злочину [1].

Розвиваючи цю ідею автори розмірковують та формулюють певну гіпотезу, що першим аналітиком за предметом аналізу злочинів, можливо, був ще кроманьйонець, який одного разу, збираючись на полювання зауважив перед своїм кланом: *«Знаєте… кожного разу, коли ми спускаємось до водопою між тим, як сонце сходить над горизонтом, і впродовж часу поки воно над нами в небі, одному з нас розбиває голову якийсь бебік з племені Великої Скали» [1].*

Важливість такого порівняння полягає в тому, що автори визначають ключовим певний процес, який відтоді мало змінився. Кроманьйонець зіставив дані (звичайно, у своїй голові, але це робить і досвідчений аналітик двадцять першого сторіччя), знайшов схему нападу при обтяжуючих обставинах, проаналізував і описав її (включно з географічними, часовими та характерними обставинами), поширив її членам свого клану та прямо рекомендував рішення. Тобто

> *за аналогією сучасного підходу до найважливіших функцій кримінального аналізу, це ні що інше як визначення «гарячих зон» для посиленого патрулювання.*

При цьому не має значення наскільки ця гіпотеза є ймовірною та виправданою.

Важливою є ілюстрація наскільки це неймовірно просто, наскільки фундаментально, наскільки нерозривними з розвитком людства є взаємозв'язки, які і сприймаються у якості джерел кримінального аналізу.

Водночас, Стівен Готліб та Шел Аренберг (*Steven Gottlieb and Shel Arenberg*) зазначили, що кримінальний аналіз направлений на виявлення підозрюваних та/або моделей злочинності можна простежити до феодального періоду Англії. Населення географічних територій було невеликим, люди добре знали один одного, і селяни часто проводили все життя в одному селі чи місті. Місцевий констебль, знав, хто такі порушники спокою, де вони живуть, і добре знав, як вони вчиняли свої злочини [2].

Важливим є виділити, при цьому, що зазначаючи про зародження кримінального аналізу, автори вказують на характерні особливості цієї діяльності: виявлення підозрюваних та визначення моделей (патернів) вчинення злочинів.

Виділення характерних особливостей кримінального аналізу тих, які і визначають його зміст, навіть в умовах сьогодення є важливим елементом.

> *Саме використовуючи історичний аналіз виникнення та розвитку кримінального аналізу як окремої інституційної складової правоохоронної діяльності, формується достатньо обґрунтоване бачення щодо методологічної бази кримінального аналізу.*

Важливим є продовження напряму історичного дослідження та з'ясування об'єктивних умов виділення кримінального аналізу в окремий професійний напрям правоохоронної діяльності. На фоні історичних періодів, які нами взяті у якості аналізу, без перебільшення можемо говорити про цивілізаційний розвиток, що пов'язаний і з науково-технічним прогресом, розвитком природничих, гуманітарних, соціальних наук, що значно сприяло і розвитку правоохоронної діяльності. Розвиток криміналістики дозволив поліцейським ідентифікувати підозрюваного, причетного до вчинення злочину, а психологія, пояснюючи природу людської особистості визначала моделі звичок правопорушників. Ці та інші

> *результати наукових досягнень дозволили правоохоронним органам точно визначити природу злочинної діяльності, передбачити її майбутні події та ідентифікувати її виконавців.*

Суспільство існує, щоб сприяти загальному добробуту своїх громадян, починаючи із забезпечення їх безпеки. Поліція є тим органом в суспільстві, основною функцією якого і є безпека громадян, а аналітики підрозділів кримінального аналізу є своєрідним головним мозком цих зусиль, що дозволяє суспільству запобігати більшості злочинів з найменшими витратами ресурсів. Звичайно, практика вивчення злочинів передує професії. Безумовно, вартові Ассирії, вартові Вавилону та вартові Риму знали про закономірності, гарячі точки та «рецидивістів». Звичайно, вони знали, на чому зосередити свої ресурси: певних місцях, часі і конкретних особах, щоб максимізувати зусилля [1].

У центрі усіх цих подій виділяється також те, що є першоосновою кримінального аналізу, і вона настільки є базовою характеристикою феномену кримінального аналізу, що знадобилося десять тисяч років від початку цивілізації до 1960-х років, щоб ця діяльність отримала назву та професію. Те, що кримінальний аналіз виник в поліцейських установах, а не в громадах, університетах чи прес-центрах, наприклад, є результатом двох факторів: близькості до необхідної інформації та близькості до іншої поліцейського професії [1].

> *Водночас кримінальний аналіз як специфічна правоохоронна діяльність має найкращі шанси та спроможності вирішити проблеми щодо аналізу моделей та тенденцій злочинності.*

Історія професійного використання кримінального аналізу на відміну від його історії формалізованої діяльності спеціальних підрозділів кримінального аналізу є дещо іншою. Початково кримінальний аналіз розвивався як певна діяльність поліцейського, незалежно від посади: патрульний, слідчий, сищик, детектив, оперативний працівник, - який в межах професійної діяльності

> *використовував певні шаблони, алгоритми діяльності, з'ясовував в межах своєї обізнаності окремі моделі (патерни) злочинної поведінки. «Неформальний аналіз злочинності, у найпростішому сенсі, виконується всіма офіцерами під час розслідування злочинів» [1].*

Оскільки кримінальний аналіз можна інтерпретувати як якісний аналіз злочину та подальше порівняння його з аналогічними минулими подіями, кожен правоохоронець, пов'язаний з розслідуванням злочину, забезпеченням правопорядку та безпеки, функціонально здійснює певний вид кримінального аналізу,

> *але результати його аналізу базуються переважно на власному досвіді і частково досвіді колег.*

Однак власний досвід є все ж таки обмеженим і не може визначатися як певна система знань в межах території, регіону або країни. Обізнаність кожного правоохоронця щодо кожного злочину, навіть в межах діяльності одного правоохоронного органу ймовірно є не повною. Вони не мають можливості порівнювати способи вчинення злочинів щодо кожного повідомлення, порівнювати з минулими випадками. Їх особистий кримінальний аналіз проводився на несистематичній основі, тому багато моделей і тенденцій залишалися невиявленими. Тому

> *об'єктивним є процес виділення серед правоохоронців окремого фахового напряму діяльності та її формалізації окремими спеціальними підрозділами – кримінального аналізу.*

Інституційне становлення кримінального аналізу в правоохоронній діяльності є процесом еволюційного характеру. Об'єктивно на фоні зростання рівня фаховості правоохоронців, і в першу чергу практиків, мова ще не йде про певні наукові узагальнення та дослідження, висунення певних теоретичних гіпотез та визначення правоохоронних моделей. Доречно говорити про

> *збільшення інформаційних потоків щодо злочинності, неспроможності узагальнення усієї інформації про злочини одним правоохоронцем, а відтак формування об'єктивної необхідності виділення в системі правоохоронної діяльності окремих спеціалізованих підрозділів, які і отримали назву у перспективі як підрозділи кримінального аналізу.*

Посилаючись на джерело «A History of Crime Analysis» [1], у створеній сером Робертом Пілом в 1829 році лондонській столичній поліції (*London Metropolitan Police*), у відділках працювало по два «детективи», і цілком імовірно, що ці перші розслідувачі використовували деякі методи сучасного кримінального аналізу, щоб зв'язати кримінальні інциденти певними закономірностями. Саме тому

> *за результатом діяльності лондонської поліції було вперше розроблено концепцію modus operandi (спосіб вчинення) та класифікацію правопорушників і злочинів на її основі.*

Modus operandi допоміг поліції точніше визначати моделі (патерни) та серійність злочинів, хоча він, на той час, застосовувався переважно до випадків вбивства.

Не дивлячись на те, що концепція modus operandi сформувала лише початкові засади упровадження професії аналітика за напрямом кримінального аналізу,

> *подальший інституційний розвиток кримінального аналізу саме на основі цієї концепції набув інноваційного характеру в підрозділах американських поліцейських.*

Період 1905-1932 рр. пов'язують з діяльністю міського маршала в Берклі (Каліфорнія) Августа Воллмера (August Vollmer) (з 1909 року цю посаду було перейменовано на «начальника поліції»). До його приходу в місті надзвичайно активними були банди мародерів і потяги, що прямували через Берклі відмовлялися там зупинятися. Але на момент, коли Воллмер залишив посаду, Берклі вважався одним із найбезпечніших міст Америки [1].

На той час Воллмер дійсно був новатором поліцейської роботи, запровадивши велосипедний та автомобільний патрулі, радіозв'язок, систему відбитків пальців. Він також

> *сприяв розвитку наукових досліджень у цій сфері, становлення поліцейської академії та школи криміналогії Каліфорнійського університету, а також визначив вимоги до вищої поліцейської освіти та професіоналізму.*

Однак набагато важливішими є його новації в кримінальному аналізі. На початку 1900-х років запровадив англійську техніку систематичної класифікації відомих правопорушень modus operandi для Сполучених Штатів. У 1906 році він керував розробкою базової системи управління даними, яка допомогла організувати поліцейські звіти у спосіб, що сприяв їх аналізу. Він заохочував регулярний перегляд поліцейських звітів для проведення аналізу частоти подій та позначав місця вчинення злочинів кольоровими шпильками, що зіграло важливу роль у просуванні використання «шпилькових» або «точкових» карт для візуального визначення територій зосередження випадків вчинення злочинів та повідомлень про них. І найважливіше, він отриману інформацію про злочини використовував у подальшому плануванні маршрутів патрулювання поліцією [1]. Коли в 1909 році Воллмер організовував роботу своїх патрульних на велосипедах, він визначав район патрулювання відповідно до очікуваної кількості викликів з конкретних районів міста. [3, с.8]

Хоча термін «кримінальний аналіз» (crime analysis) ще не був винайдений, одна цитата з публікації Воллмера «Район поліцейського патрулювання» свідчить про те, що він був знайомий із його поняттями:

> *«Припускаючи регулярність злочинів і подібних подій, можна звести ці випадки в таблицю за районами в межах міста і таким чином визначити місця, які мають найбільшу небезпеку вчинення таких злочинів, а які мають найменшу небезпеку.» [3, с.9]*

В історичному контексті, враховуючи початкові форми та засади кримінального аналізу, ключовим елементом розглядалася необхідність ретельного порівняння злочинів, вчинених у теперішній час та у минулому. Тобто аналітик зосереджує свою увагу на виявленні закономірностей та тенденцій. Звісно, що аналітик не буде витрачати час на порівняння вуличного пограбування, що має місце останнім часом, з викраденням автомобілів, що мало місце у минулому. Порівняння чи співставлення здійснюється саме однорідних злочинів, в першу чергу, хоча, враховуючи різноманітність способів вчинення злочинів, наявність самої широкої низки характерних ознак, виявлення однорідних характеристик та їх порівняння також може мати місце.

> *Таким чином, процес кримінального аналізу базується на системному використанні методів класифікації та категоризації.*

Водночас на початку сторіччя ефективних методик класифікації злочинів було небагато. Не дивлячись на те, що в основі класифікації злочинів використовувалися чинні закони, все ж кримінальне законодавство в різних штатах США суттєво відрізнялося. Крадіжка зі зломом у Каліфорнії може бути визначена значно інакше, ніж крадіжка зі зломом у Меріленді [1].

Враховуючи саме таку особливість проблеми кримінального аналізу, розпочинаючи з 1922 року, Міжнародна асоціація начальників поліції (*International Association of Chiefs of Police (IACP)*) започаткувала, певним чином, стандартизацію національної системи звітності про злочини. І вже у

1930 році була розроблена, за активної і важливої участі Воллмера – «Єдина програма звітності про злочини» (*Uniform Crime Reporting Program (UCR)*).

Для українських реалій зазначена проблема не є актуальною, саме щодо класифікації злочинів. Усі злочини в Україні кодифіковані згідно Кримінального кодексу України і це зрозуміло, що в рамках однієї держави інакше не може бути. Водночас в Україні все ж залишаються питання щодо необхідності систематизації, єдиних стандартів та стандартизації безпосередньо кримінального аналізу.

Але доповнюючи зазначені процеси удосконалення та систематизації процесів класифікації злочинів за ініціативою керівників поліції в США, подальші процеси удосконалення цієї роботи та управління програмою UCR було покладено на Федеральне бюро розслідувань, але це ніяким чином не вплинуло на погіршення умов діяльності аналітиків і було надійною базою подальшого розвитку кримінального аналізу.

Розвиток кримінального аналізу у подальшому пов'язують з діяльністю Орландо В. Вілсона (*Orlando W. Wilson (1900-1972)*) – одного із найвидатніших поліцейських реформаторів сторіччя і одночасно послідовника ідей та розробок Августа Воллмера. Вілсон розширив методику аналізу Воллмера, включивши формули небезпеки або призначення вагових коефіцієнтів для різних категорій злочинів і викликів служби, щоб забезпечити систематичний підхід до розподілу ресурсів патрулювання. Важливим є зазначити, що початково, маючи певний практичний досвід (*губернатор військової поліції в післявоєнному Берліні, начальник поліції у Фуллертоні, Каліфорнія (1925); начальник поліції у Вічіті (1928-1939)*),

Вілсон реалізував свої думки в системних публікаціях академічного характеру:
«Поліцейські протоколи» (1942),
«Поліцейське управління» (1950)
«Поліцейське планування» (1957)),

перебуваючи в посаді декана Школи кримінології Каліфорнійського університету в Берклі (школи, заснованої Воллмером) [1].

Потрібно зазначити, що Вілсон у своїх ранніх публікаціях («Поліцейське управління» (1950)) згадує про важливість виявлення моделей і тенденцій злочинності, але не пропонує формальної програми для цього, тобто не визначає відповідної інституційної форми кримінального аналізу. Але такий практичний досвід та відповідна академічна й наукова діяльність сформували цілісну систему знань Вілсона, що мало важливе значення подальшого інституційного розвитку кримінального аналізу у цілому та системного упровадження в практичній поліцейській діяльності, у період перебування у посаді суперінтенданта поліції в Чикаго (1960-1971).

Можна зазначити, що найдавніше відоме джерело терміну «кримінальний аналіз», пов'язується з наступним виданням Вілсона «Поліцейське управління» (1963). Саме у розділі «Спеціалізація в рамках великого відділу планування» *(«Specialization Within a Large Planning Division»)* ми знаходимо [4]:

> *Підрозділ кримінального аналізу вивчає щоденні звіти про серйозні злочини з метою визначення місця, часу, особливостей, подібності з іншою кримінальною діяльністю та різноманітних важливих фактів, що можуть допомогти ідентифікувати злочинця або існування схеми злочинної діяльність. Така інформація є корисною для планування діяльності підрозділу чи регіону.*

Це було вперше визначено поняття «Кримінальний аналіз». Його використання Вілсоном свідчить про формалізоване існування підрозділів кримінального аналізу на момент написання.

Тобто на практиці така специфічна діяльність інституційно вже була сформована у формі певного окремого підрозділу кримінального аналізу.

Наприкінці 1960-х років у великих поліцейських організаціях країни почали створювати підрозділи аналізу злочинів. Ці підрозділи в першу чергу відповідали за виявлення методів злочинної діяльності, виявлення моделей злочинності в межах географічних районів і визначення зв'язків між відомими правопорушниками [5].

А до опублікування у 1972 році наступного видання «Поліцейське управління», важливість кримінального аналізу настільки зросла, що Вілсон присвятив йому кілька сторінок щодо адміністративних питань та системних обов'язків підрозділу,

> *визначаючи кримінальний аналіз функцією планування та рекомендуючи створити сектор кримінального аналізу у відділі планування великого агентства [6].*

Хоча більш пізні тексти рекомендували відокремити кримінальний аналіз від планування та адміністрування.

Таким чином, «Поліцейське управління» Вілсона стало першим підручником для керівників поліції (і залишається ним сьогодні). «Crime analysis» (кримінальний аналіз) став модним словосполученням, як «community policing» стала в 1990-х роках. Без сумніву, книга Вілсона допомогла прокласти шлях до буму кримінального аналізу у 1970-х роках [1].

На фоні зростання рівня злочинності у цей період та, враховуючи важливий внесок у розвиток кримінального аналізу Воллмера та Вілсона, сформувалась достатня критична маса фахівців та розуміння необхідності використання кримінального аналізу в практиці поліцейської діяльності. А тому подальша генерація, підживлення ідей та системи кримінального аналізу відбувалася на основі колективної професійної спільноти, тобто сформованих спільних ініціатив як фахівців кримінального аналізу так і різного роду ініціатив держави.

Розвиток кримінального аналізу набуває нового поштовху на основі сприйняття суспільством його ефективності у протидії злочинності та відповідним реагуванням законодавця:

- ✓ *(Закон про допомогу правоохоронним органам (Law Enforcement Assistance Act) (1965);*
- ✓ *Закон «Омнібус про безпечні вулиці та контроль злочинності» (Omnibus Safe Streets and Crime Control Act) (1968));*

розвитком цілеспрямованої ініціативи у формі фондів, асоціацій та організацій:

- ✓ *Law Enforcement Assistance Administration (LEAA) (1968);*
- ✓ *Integrated Criminal Apprehension Program (ICAP) (1970);*
- ✓ *International Association of Crime Analysts (1990);*
- ✓ *Bureau of Justice Assistance (1994);*
- ✓ *National Institute of Justice (1994);*
- ✓ *Massachusetts Association of Crime Analysts (1997).*

з метою додаткового фінансування інновацій в правоохоронній діяльності, наукового освітнього та методичного забезпечення та узагальнення практики, зокрема і щодо інституційного закріплення та удосконалення форм і методів кримінального аналізу.

Перш за все, необхідно виділити Міжнародну асоціацію начальників поліції (*International Association of Chiefs of Police (IACP)*), агентство, яке займається наданням фінансової допомоги різним програмам боротьби зі злочинністю (*Law Enforcement Assistance Administration (LEAA)*) та Інтегровану програму затримання злочинців (*Integrated Criminal Apprehension Program (ICAP)*). Цей період характеризувався упровадженням великої кількості нових програм, спрямованих на зниження рівня злочинності.

Як зазначено в літературі «Гроші хлинули з LEAA, як вода з пожежної станції, і багато агентств опинилося у фондах» [1].

У Сполучених Штатах з'явилися сотні відділів кримінального аналізу, деякі з них – у великих агентства, яким вони були гостро потрібні, але й багато в менших агентствах, які інакше не змогли б собі їх дозволити.

Агентство, яке займалося наданням фінансової допомоги різним програмам боротьби зі злочинами фінансувало видання низки навчальних посібників та довідників для аналітиків, зокрема: Посібник відділу кримінального аналізу поліції (Національний інститут правоохоронних органів і кримінального правосуддя, 1973); Керівництво з кримінального аналізу (1977); Аналіз патрульних операцій (1977); Кримінальний аналіз на підтримку патрульних (1977) тощо. І як результат, Національна консультативна комісія зі стандартів і цілей кримінального правосуддя (*National Advisory Commission on Criminal Justice Standards and Goals*) рекомендувала можливість створення відділу кримінального аналізу у кожному поліцейському відомстві.

На розширення кримінального аналізу та спеціальне його виділення також вплинула розробка Інтегрованої програми затримання злочинців (ICAP) Агентством, що надавало допомогу правоохоронним органам (LEAA) у 1970-х роках. Започаткована президентом Річардом М. Ніксоном, ця федеральна організація була створена на основі Закону «Омнібус про безпечні вулиці та контроль злочинності», і програма базувалася на концепції, що багато проблем зі злочинністю можна приписати особам, які вже є відомими злочинцями або, принаймні, рецидивістам.

Засновники програми ICAP визнали, що люди, які присвятили себе кримінальному способу життя (кар'єрні злочинці), часто будуть у полі зору представників правоохоронних органів. Іноді їх арештовували і складали протокол про арешт. В інших випадках вони можуть бути об'єктом профілактичного заходу, дільничного обходу, або попасти у запис дорожньо-транспортної пригоди. У кожному випадку поліцейські включали б у свої документи фізичний опис особи, її адресу, опис транспортного засобу (якщо необхідно) і запис про те, як був вчинений злочин (modus operandi). Однак до епохи комп'ютеризації ця інформація мала невелику цінність, оскільки все, що стосувалося особи, зазвичай було зорієнтовано на прізвище та ім'я суб'єкта.

Офіцери могли реагувати на місця злочину та отримувати описи підозрюваних, але, оскільки вони не мали імені та прізвища, то не могли отримати і доступу до відомчих записів на предмет можливих збігів. Вони могли виявити певні шаблони МО (modus operandi), але без імені підозрюваного не могли шукати у файлах, раніше заарештованих осіб, які використовували ті самі шаблони МО.

ІСАР намагався переробити системи ведення записів поліцейських установ і краще використовувати величезні обсяги даних, зібраних бюро записів. Завдяки цим змінам поліцейські сьогодні можуть записувати фізичні описи підозрюваних і на їх підставі з'ясовувати імена підозрюваних за допомогою комп'ютера. Подібним чином можна вводити шаблони МО та порівнювати їх із тими, які використовували підозрювані, яких раніше заарештовували.

ІСАР також зазначав, що рецидив часто є породженням звички. Такі особи часто вчиняють злочини в один і той же час, дні тижня, або тим же методом. Тому ІСАР рекомендував створити відділи кримінального аналізу для моніторингу тенденцій і закономірностей та повідомляти про це патрульним підрозділам та персоналу слідства. Крім того, було рекомендовано розробляти цілеспрямовані планів патрулювання у якості тактичних дій щодо вирішення проблем, на які звертає увагу відділ кримінального аналізу.

Ці концепції, а також інші, виведені зі знаменитого дослідження департаменту поліції Канзас-Сіті 1970-х років, завдали смертельного удару освяченій часом традиції виставляти поліцейські підрозділи за теорією «випадкового патрулювання» [6, с. 9]. Протягом багатьох років вважалося, що видима присутність поліцейських є суттєвим стримуючим фактором для злочинності, і найкращим способом вирішення проблеми злочинності є найняти більше поліцейських. Підтримувати цю віру було дорого; що більш важливо, це виявилося неправдою [6, с. 9].

Дослідження в Канзас-Сіті показало, що найважливішим було не те, скільки співробітників має агентство, а те, що вони робили з цими співробітниками. Якби агенція розмістила своїх офіцерів у східній частині міста, а всі її шахраї – у західній, мало що можна було б досягти у зниженні злочинності. Таким чином, у дослідженні було зроблено висновок, що найкраще використання патрульної сили було досягнуто, коли поліцейські були розміщені в потрібних місцях у потрібний час. Згодом відділ кримінального аналізу став розглядатися як той компонент департаменту, який міг би надати значну допомогу патрульним поліцейським.

Оскільки все більше агентств почали приймати цю концепцію, накопичилися додаткові докази, що випадкове патрулювання дорівнює випадковим результатам. Замість зосередження на придбанні ресурсів концентрація була перенаправлена на правильний розподіл ресурсів. Офіцери більше не будуть сідати в патрульну машину, їздити тридцять років, а потім йти на пенсію. З цього моменту інспектори керуватимуться у своїй діяльності інформацією, наданою їм підрозділом кримінального аналізу.

Відповідно до програми ІСАР ця концепція стала базовою щодо управління патрульними операціями (*«Management of Patrol Operations» (MCI)*). Крім того, Програма підтримала інші зміни, які також призвели до кращого використання патрульних ресурсів. Офіцери мали змогу зосереджуватися на запобіганні злочинів і затриманні злочинців, використовувати системи пріоритетності повідомлень, системи повідомлень поштою тощо.

Крім того, в рамках ІСАР МСІ прагнуло покращити якість підготовки справ, подальший розвиток відносин між поліцією та прокуратурою, виявлення професійних злочинців, а також збільшення кількості та частки заарештованих. У той же час, МСІ було розроблено для забезпечення ефективності розслідування злочинів за участю патрульних. ІСАР рекомендував посилити процедури перевірки випадків і включення факторів розкриття в попередні звіти про злочини. Патрульних поліцейських заохочували повноцінно брати участь у початкових розслідуваннях, отримуючи максимум інформації, яку можна було отримати під час перших контактів поліцейських із потерпілими та/або свідками. Нарешті, Програма ІСАР рекомендувала, щоб відділи кримінального аналізу надавали слідчим інформацію про підозрюваних, аналіз моделей МО та інші подібні засоби, щоб допомогти агентству ідентифікувати злочинців і можливі майбутні місця злочинної діяльності.

Розвиток кримінального аналізу відбувався переважно внаслідок діджиталізації світової поліциїстики. Лише з 1980-х років значна частина поліцейських виявила спроможності щодо використання даних статистичних обліків не лише для щорічних підсумків частот злочинів. Навіть поряд з цим, відсутність відповідних комп'ютерних апаратних засобів та програмних продуктів неминуче гальмували зростання галузі кримінального аналізу [7, с. 179]. Лише за останні десятиріччя набуло широкого розповсюдження створення різноманітних продуктів для кримінального аналізу представниками бізнесу, які успішно конкурують з найнятими правоохоронними органами програмістами або контрактами з університетами. Це зростання сформувало професійну сферу кримінального аналізу.

Незважаючи на наступний період певного затухання розвитку кримінального аналізу, а 1980-ті роки характеризувалися зниженням фінансування та ліквідацією окремих підрозділів кримінального аналізу, 1990-ті роки вважаються періодом ренесансу кримінального аналізу. Цей період нового поштовху до розвитку кримінального аналізу пов'язують з виходом книги «Проблемно-орієнтована поліцейська діяльність» (ПОП) (*Problem-Oriented Policing (POP)*) професора Університету Вісконсіна Германа Гольдштейна (*Herman Goldstein*), який був свого часу помічником О. В. Вілсона в поліції Чикаго з 1960 по 1964 рік. Розвиваючи ідеї кримінального аналізу на принципах вирішення проблем та запобігання злочинам, в США з'являються сотні нових програм розвитку кримінального аналізу з новим фінансуванням. На той час ПОП була інноваційною моделлю поліцейської діяльності і тому дуже бурхливо розвивалася і тисячі агентств прийняли програми та принципи ПОП. Проблемно-орієнтована поліцейська діяльність описує набір процедур, спрямованих на підвищення ефективності поліцейських операцій шляхом зосередження уваги на проблемі злочинності загалом, а не на окремому злочині, і на способах усунення причин, що в основі прояву злочинності. Як пояснює сам Гольдштейн,

> *«розглядаючи інциденти, поліцейські зазвичай мають справу з найбільш очевидними, зовнішніми проявами глибшої проблеми, а не з самою проблемою. Вони можуть припинити бійку, але не брати участь у дослідженні факторів, які сприяли цьому... Вони можуть розслідувати злочин, але не досліджувати чинники, які могли сприяти його вчиненню, за винятком тих випадків, коли вони стосуються ідентифікації правопорушника...» [8, с. 33].*

Саме з сутності ПОП і очевидними є завдання для кримінального аналізу: розв'язання проблеми злочинності базується на першочерговому виявленні та аналізі аналітиками підрозділів кримінального аналізу.

Аналіз злочині є основою, на яку поліція може опиратися, щоб задовольнити набагато ширші та глибші вимоги щодо розслідування, пов'язаного з проблемно-орієнтованою поліцейською діяльністю. У поліцейському відомстві, в якому окремі офіцери можуть не знати, що сталося за межами районів, де вони працюють, або в періоди, коли вони не перебувають на службі, кримінальний аналіз був основним засобом для об'єднання інформації, яка може допомогти розкрити злочини...

> *Орієнтована на проблему поліцейська діяльність фактично створює стимул для більш ефективного використання даних, які зазвичай збираються в процесі кримінального аналізу» [8, с. 37].*

Нового поштовху до розвитку професія аналітика у сфері кримінального аналізу набула з 1990 року, з року заснування Міжнародної асоціації аналітиків злочинності (*International Association of Crime Analysts (IACA)*), заснованої з метою обміну інформацією та ідеями, відстоювання професійних стандартів та можливості фахового навчання. IACA організовує та проводить щорічні конференції для аналітиків, акцентуючи увагу на професійних тренінгах з кримінального аналізу. Але найбільшим досягненням таких конференцій є можливість спілкування сотень аналітиків, обмінюватися досвідом, ідеями щодо використання нових методів та засобів кримінального аналізу.

З цього часу почався новий тип фінансування поліцейської діяльності взагалі, і кримінального аналізу, зокрема, особливо у період президента Клінтона, який забезпечив введення 100 тисяч нових посад в поліції. Цей період також супроводжувався створенням низки недержавних професійних об'єднань аналітиків у сфері кримінального аналізу.

Крім того 1990-і роки характеризуються суттєвими технологічними досягненнями, що використовувалися у поліції. Відповідне федеральне фінансування сприяло залученню технологічно нового інструментарію для обробки текстів, обробки чисел, управління базами даних, картографування злочинності комунікації та презентацій тощо, що дозволило кримінальному аналізу стати набагато ефективнішим. У цей же період (1994 р.) з'являється нова модель поліцейської діяльності «Comstat», запроваджена Департаментом поліції Нью-Йорка та, яка базується на кримінальному аналізі, формуванні мапи злочинності та розробці відповідної стратегії. Цьому також сприяло те, що у першій половині 90-х років дві компанії – ESRI (Інститут дослідження систем навколишнього середовища) і MapInfo – представили перші програми для мапування злочинності, доступні для аналітика як з точки зору вартості, так і з точки зору технології. І з цього часу мапування злочинності більше не було наклеюванням кольорових наліпок на паперові карти.

У подальшому терористичні напади 11 вересня 2001 року в США і подальша війна з тероризмом охопили навіть агентства місцевого рівня, змістивши пріоритети і фокус з традиційного кримінального аналізу на розвиток аналітичної розвідки для забезпечення внутрішньої безпеки [9, с. 5].

> *Кримінальний аналіз, з його традиційним акцентом на вуличних злочинах та інших питаннях, що є проблемою органів влади місцевого рівня, повернувся на шлях адаптації до нової парадигми – INTELLIGENCE.*

Таким чином, інституційне становлення кримінального аналізу достатньо обґрунтовано характеризується відповідною історичною ретроспективою, яка розкриває його сутнісні характеристики та етапи еволюційного розвитку.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *A History of Crime Analysis*. Retrieved from https://faculty.uml.edu//jbyrne/44.203/maca-historyofcrimeanalysis.pdf
2. Steven, Gottlieb & Shel, Arenberg (1992). *Crime Analysis: From Concept to Reality*/ Office of Criminal Justice Planning Edition.
3. *Crime Analysis in Support of Patrol* (1977). National Institute of Law Enforcement and Criminal Justice, Law Enforcement Assistance Administration, U.S. Department of Justice.
4. Orlando W., Wilson & Roy, McLaren (December 1, 1963). *Police Administration*. McGraw-Hill Education; 2Rev Ed edition.
5. Richard, G. Grassie (April, 1977). *Crime Analysis Executive Manual.* U.S. Depanment of Justice. Law Enforcement Assistance Administration.
6. Gottlieb, Steven, et. al. (1994). *Crime Analysis*: from First Report to Final Arrest. Alpha Publishing,
7. Christopher, S. (2004). *A practitioner's perspective of UK strategic intelligence*. In J. H. Ratcliffe (Ed.), Strategic Thinking in Criminal Intelligence (First ed.). Sydney: Federation Press.
8. Goldstein, Herman (1990). *Problem-Oriented Policing*. New York: McGraw-Hill.
9. *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, KS.

DOI: https://doi.org/10.36486/978-966-2310-66-5-10

Здатність до аналізу не слід змішувати з простою винахідливістю, бо аналітик завжди винахідливий, тоді як не кожна винахідлива людина здатна до аналізу.

Едгар Аллан По

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

Дмитро Овсянюк

Кримінальний аналіз, як мультидисциплінарна інформаційно-аналітична діяльність широко використовується провідними правоохоронними органами світу для підвищення ефективності протидії злочинності, забезпечення раціонального використання ресурсів та обґрунтованого управління. Кримінальний аналіз є основною складовою моделі поліцейської діяльності, керованої аналітичною розвідкою (Intelligence-led Policing (ILP)), яка спрямована на підтримку інституційного управління та рішень слідчих й оперативників на основі процесу аналізу інформації та поширення аналітичних висновків.

В певній частині кримінальний аналіз використовувався в органах внутрішніх справ України задовго до створення відповідних аналітичних підрозділів, разом з тим, це часто носило несистемний та неврегульований характер. Серед елементів сучасного кримінального аналізу, що використовувались в ОВС слід відмітити наступні: аналіз оперативної обстановки та прогнозування її розвитку, встановлення тенденцій злочинності, аналіз структурованої інформації з використанням аналітичних інструментів, пошук інформації у відкритих джерелах, комплексний аналіз інформації здобутої з різних джерел у ході досудового розслідування або оперативно-розшукової діяльності, створення автоматизованих інформаційно-пошукових систем на основі інтегрованих банків даних, тощо [1].

У своєму сучасному розумінні, як системна діяльність, що є частиною моделі поліцейської діяльності керованої аналітичною розвідкою, кримінальний аналіз впроваджувався в МВС відповідно до рекомендацій міжнародних партнерів України з урахуванням передового правоохоронного досвіду.

Серед перших ініціатив з впровадження кримінального аналізу в МВС необхідно згадати про Проєкт «Розвиток системи кримінального аналізу та аналізу ризиків, сумісної зі стандартами ЄС, в структурах правоохоронних органів України, які протидіють злочинам, що пов'язані з торгівлею людьми», який реалізовувався протягом 2014-2016 років Представництвом Міжнародної організації з міграції в Україні за підтримки Бюро з міжнародних питань у сфері боротьби з незаконним обігом наркотиків та правоохоронних питань Державного департаменту США. В проєкті, серед іншого використовувався досвід Державної прикордонної служби України щодо розбудови кримінального аналізу, працівники якої, а також автор, увійшли до складу робочої групи експертів з впровадження кримінального аналізу. Варто зазначити, що першими на теренах України визнали необхідність виділення кримінального аналізу в окремий напрямок саме у Державній прикордонній службі України.

У січні 2016 року презентовано Експертний звіт щодо запровадження системи кримінального аналізу та аналізу ризиків, сумісної зі стандартами ЄС, підготовлений представниками Міжнародної організації з міграції (далі – МОМ) в Україні, експертами Адміністрації Держприкордонслужби та ДБЗПТЛ.

Проєкт започаткував практику кримінального аналізу в підрозділах боротьби зі злочинами, пов'язаними з торгівлею людьми, зміцнив потенціал служби у протидії злочинності та заклав фундамент створенню відділу кримінального аналізу у структурі Департаменту інформаційної підтримки та координації поліції «102» (далі – ДІПКП «102»), як підрозділу-координатора напряму, а також, в подальшому, сектору кримінального аналізу в складі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми (станом на 2023 рік – Департамент міграційної поліції).

08 квітня 2016 року наказом Національної поліції створено відділ кримінального аналізу, який запрацював у структурі Департаменту інформаційної підтримки та координації поліції «102». На

перших етапах підрозділ виконував адміністративні функції, адаптувався під вимоги часу та потреби служб, був малочисельний, а у положенні про ДІП КП «102» узагалі були відсутні завдання та функції щодо проведення кримінального аналізу.

Важливу роль у впровадженні концепції ILP в Національній поліції України відіграла Консультативна місія Європейського союзу в Україні (далі – КМЄС). 04.11.2016 за ініціативи КМЄС, з метою напрацювання пропозицій щодо проведення поглибленої оцінки потреб і підготовки адаптованого рішення, необхідного для реалізації в Національній поліції концепції «Intelligence-led Policing» та забезпечення взаємодії зі співробітниками Консультативної місії Європейського Союзу в Україні з цього питання, наказом НПУ № 1132 створено робочу групу з напрацювання пропозицій до концепції «Intelligence-led Policing». Попередня оцінка потреб впровадження ILP в Національній поліції України була здійснена КМЄС у червні-липні 2016 року шляхом проведення консультацій з представниками департаментів кримінальної поліції, а також інформаційно-аналітичної підтримки, організаційно-аналітичного забезпечення та оперативного реагування, патрульної поліції та превентивної діяльності Національної поліції України. У результаті зустрічей були визначені основні прогалини в поточній національній моделі поліцейської діяльності та запропоновано МВС та НПУ створити робочу групу для напрацювання відповідних пропозицій, про що було вказано вище [2].

Протягом листопада-грудня 2016 року, КМЄС спільно з міжнародними експертами-аналітиками проведено оцінку потреб щодо впровадження моделі ILP в межах НПУ, про що складено відповідний звіт, який був переданий до МВС та НПУ. Рекомендації звіту стали дорожньою картою першопочаткових заходів з подальшої розбудови кримінального аналізу в поліції. Серед іншого у звіті міститься рекомендація створення на національному рівні єдиного незалежного структурного підрозділу з питань аналізу, який зможе забезпечити координування діяльності з впровадження моделі ILP (Центральний департамент аналізу), рекомендації щодо відбору, підготовки аналітиків, перегляду ІТ інфраструктури, ролі КМЄС у розбудові аналітичних можливостей НПУ та МВС тощо.

Наступним важливим кроком розбудови кримінального аналізу в НПУ стало створення, відповідно до наказу від 20 липня 2017 року № 735, окремого Управління кримінального аналізу (у складі кримінальної поліції), головним завданням якого стала організація та здійснення інформаційно-пошукової та інформаційно-аналітичної роботи для реалізації повноважень поліції. З метою впровадження системи кримінального аналізу в діяльність Національної поліції України, методів ILP та визначення основних напрямів діяльності Управління кримінального аналізу Національної поліції України 18 серпня 2017 року наказом НПУ № 875 створено робочу групу з розвитку та впровадження системи кримінального аналізу в Національній поліції України, до складу якої, серед інших, входив автор. Більше того, 11 грудня 2017 року керівництвом НПУ затверджено «План упровадження методів та принципів «Intelligence-led Policing» до інформаційно-аналітичної роботи Національної поліції України у 2017 - 2018 роках».

У процесі реформування кримінального блоку Національної поліції, запровадження новітніх підходів до організації протидії тяжким, особливо тяжким злочинам та їх попередження, спираючись на рекомендації з указаних питань КМЄС та відповідно до вимог Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року затверджено Перелік змін у штатах Національної поліції, відповідно до якого реорганізовано Управління кримінального аналізу та створено Департамент кримінального аналізу чисельністю в 51 штатну посаду.

Відповідно до Положення про Департамент кримінального аналізу (далі – Департамент, ДКА) на Департамент покладено завдання з проведення, організації та координації інформаційно-пошукової та аналітичної роботи, спрямованої на збір, оцінку та реалізацію інформації, у тому числі інформації з обмеженим доступом, шляхом надання її уповноваженим органам (підрозділам) для вжиття заходів відповідно до їх компетенції, оцінювання ризиків, а також використання її для забезпечення виконання функцій, покладених на поліцію.

2020 рік мав важливе значення для подальшого розвитку та впровадження концепції ILP, а також поширення напрацьованого досвіду щодо застосування кримінального аналізу у протидії злочинності на місцевий рівень.

12 березня 2020 року Головою Національної поліції України підписано наказ № 202, яким передбачено створення підрозділів кримінального аналізу в структурі територіальних органів поліції, і вже 10 червня 2020 року наказом № 424, затверджено штатні структури підрозділів кримінального аналізу в головних управліннях Національної поліції в областях та м. Києві кількістю 232 штатні одиниці.

02 липня 2020 року відповідно до наказу МВС № 504 Департамент перебрав функцію забезпечення формування і підтримки функціонування автоматизованої інформаційної системи оперативного призначення, що формується в процесі здійснення агентурної, оперативно-розшукової та аналітичної діяльності.

Для покращення якості та практичної спрямованості підготовки фахівців з кримінального аналізу та інформаційно-аналітичної діяльності, співпраці Департаменту кримінального аналізу з Національною академією внутрішніх справ (далі – НАВС, академія) 07.07.2020 на засіданні Вченої ради НАВС прийнято рішення про створення в академії Центру кримінальної аналітики. 21.08.2020 наказом НАВС № 677 оголошено перелік змін у штаті НАВС та створено аналітичний відділ (Центр кримінальної аналітики), який за участі кафедр інформаційних технологій та кібербезпеки, оперативно-розшукової діяльності та економічної безпеки НАВС забезпечує підготовку майбутніх аналітиків, підвищення кваліфікації працівників підрозділів кримінального аналізу, здійснює заходи щодо популяризації кримінального аналізу серед правоохоронців та розробляє його методику.

Висока ефективність роботи підрозділів кримінального аналізу в складі Головних управлінь Національної поліції (далі – ГУНП) сприяла тому, що досвід створення таких підрозділів було поширено на рівні районних управлінь поліції. Зокрема, в місті Києві сектори кримінального аналізу створено в усіх в районних управліннях поліції. Загалом станом на 2023 рік функціонують понад 30 секторів кримінального аналізу у районних управліннях поліції (далі – РУП), а у багатьох РУП за ініціативи їх керівників закріплено окремих працівників, що виконують функції кримінальних аналітиків.

За час свого існування підрозділи кримінального аналізу продемонстрували свою ефективність і внесли значний вклад у безпеку країни. ДКА продовжує розвивати концепцію ILP, впроваджуючи сучасні інструменти і методи аналізу для покращення спроможностей поліції ефективно виконувати свої обов'язки, зокрема у період воєнного стану.

Працівники ДКА активно долучаються до документування воєнних злочинів агресора, проводять роботу з ідентифікації воєнних злочинців та колаборантів, встановлюють постраждалих, приймають участь у розслідуванні складних, резонансних та багатоепізодних справ, проводять стратегічний та тактичний аналіз для виявлення тенденцій злочинності та запобігання їй.

Кримінальний аналіз є основою ILP моделі, яка спрямована на інтеграцію інтелектуальних аналітичних підходів у правоохоронну діяльність, підвищення ефективності правоохоронних органів, шляхом збільшення ролі аналітичної розвідки в процесі прийняття рішень та планування. Така діяльність серед іншого вимагає наявності висококваліфікованих працівників, які володіють необхідними навичками та знаннями [3].

Разом з тим, не зважаючи на зростаючий запит правоохоронних органів України на працівників, що володіють компетентностями у сфері інформаційних технологій та кримінального аналізу, на сьогодні, відсутнє єдине бачення щодо необхідного рівня знань, навичок, досвіду, якостей та інших характеристик, які потрібні для ефективного виконання таких обов'язків.

Наявність такого бачення, зокрема у формі профілю професійної компетентності, є важливим для створення стандартизованого освітнього фреймворку, розроблення та впровадження ефективних програм навчання та підвищення кваліфікації відповідно до сучасних вимог та технологій, забезпечення практичної орієнтації та відповідності до вимог роботодавців, підвищення готовності випускників до виконання посадових обов'язків, формування професійної спільноти кримінальних аналітиків. Профіль професійної компетентності - комплексна характеристика посади, що містить визначення змісту виконуваної за посадою роботи та перелік спеціальних знань, умінь і навичок, необхідних працівнику для якісного виконання посадових обов'язків.

Отже, виникає необхідність визначення обсягу знань та навичок необхідних для виконання завдань, які стоять перед аналітиками, зокрема в поліції, ґрунтуючись на міжнародній практиці та рекомендаціях.

З моменту офіційного надання аналітикам відповідних повноважень для роботи в підрозділах поліції не вщухали дискусії щодо виокремлення навичок та компетенцій, необхідних для забезпечення ефективного виконання ними поставлених завдань. Часто ці дискусії «підсилювалися» заявами деяких керівників підрозділів про необхідність забезпечення певного рівня взаємозамінності для персоналу підрозділу. Принаймні у теорії, взаємозамінність окремих категорій співробітників значно збільшує професійну адаптивність та гнучкість в умовах відсутності розширеного штату. Персонал може бути залучений до процесу розслідування (первинний етап) та аналізу (накопичення даних). Хоча взаємозамінність і приносить певну користь для керівників та забезпечує простішу координацію, коли мова йде про оперативних працівників та аналітиків повної взаємозамінності досягти неможливо – оперативні працівники навряд чи досягнуть відповідного рівня аналітичної майстерності, а професійні аналітики навряд чи зможуть опанувати навички досвідченого опера. Максимальна ефективність аналітичної роботи не передбачає наявності попереднього досвіду правоохоронної діяльності у таких фахівців [4; 5].

У 1998 році Федеральне бюро розслідувань поширило перелік «основних компетентностей аналітиків», які були визначені стандартом для всіх аналітиків, незалежно від їх призначення та функцій;

до переліку були включені: аналіз; судження; дослідження; письмова та усна комунікація; робота з комп'ютерною технікою; професіоналізм / кооперація; гнучкість / адаптивність; здатність до навчання; ініціатива / мотивація; організація; планування та визначення пріоритетів; орієнтування у поточній ситуації; навички коучингу [6].

Незважаючи на теоретичні дискусії щодо залучення оперативних працівників до процесів аналітичної роботи, взаємодії їх з аналітиками, набагато важливішим є забезпечення опрацювання зібраної інформації досвідченими аналітиками [7, с. 15-16]. В наш час правоохоронні органи наймають аналітиків для вирішення конкретних потреб підрозділів, таких як підтримка спецоперацій у боротьбі з тероризмом, або осіб з відповідною академічною підготовкою для виконання аналітичних завдань. Все частіше правоохоронні органи визнають необхідність залучення персоналу з особливими знаннями, а це означає, що підходи до відбору персоналу повинні бути гнучкішими.

Більшість правоохоронних органів не мають можливості працевлаштовувати аналітиків для виконання спеціальних завдань подібно до того, як це організовується у розвідувальних службах. В ідеальному варіанті аналітики будуть спеціалізуватися на таких комплексних сферах як фінансові злочини, вуличні банди або інші аспекти діяльності організованих злочинних груп, які мають найбільший вплив на їх юрисдикцію. Натомість, дуже поширеною є ситуація, коли аналітик повинен зосередитися на розвитку професійних навичок і підтримці пріоритетів агенції, незалежно від того, якими вони є. Від аналітиків вимагається бути здатними до швидкого опанування нових знань, розуміти сутність досліджуваного предмета та застосовувати свої навички з урахуванням специфіки кожної проблеми.

Боротьба з окремими видами злочинності вимагає застосування додаткових заходів – з огляду на складність залучення аналітика загального профілю може виявитися недостатнім. Це не означає, що такий фахівець не може забезпечити отримання підрозділом необхідних даних, але виконання спеціальних завдань не може бути просто додатковим пунктом у переліку типових обов'язків. Аналіз даних, зібраних під час розслідування таких злочинів, як шахрайство, маніпуляції з цінними паперами, відмивання грошей, а також втручання в бухгалтерські операції потребує аналітика зі спеціальною підготовкою та досвідом.

Наприклад, висококваліфіковані фахівці - судові експерти та спеціалісти з комп'ютерної експертизи - можуть бути залучені до інтерпретації інформації та передачі даних про діяльність злочинних мереж. Менеджер підрозділу повинен визначити, чи має він ресурси для цього рівня аналізу, або чи є необхідність запрошувати аналітиків з інших агентств, що спеціалізуються на вказаних вище аспектах. Ефективність такого підходу буде залежати від характеру необхідного аналізу. Оптимальним варіантом може бути тимчасове залучення персоналу з іншого правоохоронного органу або працевлаштування фінансового аналітика, який працюватиме за сумісництвом в іншому агентстві. Спеціалізовані галузі, що включають технології та фінанси, вимагають доступу до досвіду та кваліфікації, який неможливо забезпечити в умовах дрібного масштабу. Інвестиції в розвиток таких регіональних ініціатив для невеликих агенцій є найкращим варіантом, оскільки фахівець з більшою ймовірністю буде працевлаштований кількома агентствами і, надаючи послуги декільком установам, може обійтися у меншу суму кожній із них – таким чином, фахівець матиме гідну зарплату і можливість використовувати свої знання та досвід.

Іншим варіантом оформлення трудових відносин є залучення контрактних працівників або консультантів для вирішення конкретних завдань, що потребує досвіду, відсутнього в персоналу правоохоронних органів. Останнє слово в таких випадках за законодавством, яке визначає можливість укладення таких контрактів і працевлаштування на тимчасовій основі.

Існують також різні типи досліджень і аналізу, які не можуть бути безпосередньо пов'язані зі злочинними діями, але необхідні для вироблення стратегії протидії організованій злочинності. Такий аналіз може успішно провести фахівець, найнятий за умовами контракту чи в якості консультанта.

Хоча академічне середовище може забезпечити надання цінної підтримки аналітичному підрозділу, до оформлення будь-яких домовленостей треба вирішити три ключові питання в контексті аналітичної діяльності: безпека, підзвітність і об'єктивність. Будь-який компроміс у цьому випадку може стати причиною появи проблем у всіх учасників [8].

По-перше, керівник підрозділу повинен займатися питаннями безпеки. Незалежно від специфіки проекту, особа повинна бути суб'єктом базового розслідування. Масштаб будь-якого розслідування повинен бути пропорційним до рівня конфіденційності інформації, до якої людина матиме доступ. Хоча деякі кандидати можуть проходити перевірку готовності відповідати на аналітичні виклики, питання, пов'язані з попередніми арештами або навіть маніпуляціями чи обманом у науковій сфері, повинні бути розкриті перед наданням доступу до конфіденційної інформації чи можливості відвідування засекречених об'єктів. Угоди про нерозголошення повинні бути встановлені в якості стандартної вимоги для будь-якого працівника підрозділу кримінальної розвідки правоохоронного органу.

Друге питання - підзвітність. Якщо професор погоджується надавати аналітичні послуги для підтримки операцій підрозділу кримінальної розвідки, то з самого початку слід чітко визначити очікування керівництва та скласти графік з урахуванням основного навантаження у навчальному закладі. Підрозділ повинен також намагатися дотримуватися цього графіку, незважаючи на непередбачувані обставини, які часто перешкоджають ефективному виконанню операції. Крім домовленостей щодо очікувань від обох сторін, керівництво підрозділу також повинно усвідомити, що наукові співробітники не є його прямими підлеглими – це теж потрібно враховувати перед тим, як укласти будь-яку угоду. Найкращим варіантом для забезпечення підзвітності є надання професором підтримки проекту, який може бути опублікований, для їхньої користі, при цьому залучаючи їх до завдань підрозділу або за умови отримання ними відповідної оплати після завершення.

Третє питання - об'єктивність. Є вчені, які побудували свою репутацію, отримуючи досвід на попередніх посадах та формуючи свій професійний кругозір. Керівництво підрозділу повинно бути обізнаним із особливостями досвіду наукових співробітників, оскільки це може мати безпосередній вплив на їхню майбутню роботу. Відкриті обговорення та діалог можуть, звичайно, мінімізувати ризик появи будь-яких упереджень, але доведено, що в межах розвідувальної спільноти боротися з упередженнями дуже важко людині, яка перебуває «у вакуумі». Важливо, щоб професор розуміли, які методи можливо використати для попередження можливих упереджень, такі як «аналіз конкуруючих гіпотез», який можна використати для забезпечення об'єктивності аналізу. Це не є аргументом проти розробки такого типу відносин з академіками, але з тим, що необхідно вирішити для того, щоб забезпечити, щоб робота була корисною для підрозділу.

Для того, щоб розвивати взаємовигідні відносини з членами академічної спільноти, повинна бути забезпечена можливість отримання вигоди обом сторонам. Таким чином, відносини можуть обмежуватися лише загальними (з мінімальним рівнем конфіденційності) проектами та операціями, оскільки науковці можуть мати бажання опублікувати свої методи та висновки. До тих пір, поки є можливість заздалегідь окреслити параметри проекту і в обох сторін є змога отримати вигоду, такі відносини дійсно є взаємовигідними: наприклад, можуть бути обговорені інші преференції для обох сторін, такі як отримання доступу до проектів національної безпеки або працевлаштування після завершення навчання [9]. Цінний практичний досвід, який науковці можуть отримати в рамках обраної сфери досліджень, може бути надзвичайно важливим і стимулювати розвиток таких відносин.

БАЗОВІ АНАЛІТИЧНІ НАВИЧКИ

Хоча існує широкий спектр аналітичних методів і продуктів, які відображають аналітичну діяльність, основою цього процесу є відповідний набір навичок, зокрема логічне мислення, дослідження та подання інформації у письмовому вигляді, комп'ютерна грамотність та візуалізація [10, с.6], а також критичне мислення. Аналітичні характеристики включають наполегливість, здатність до автономної роботи, гнучкість і готовність робити певні судження [10, с.6]. Інші, не менш важливі характеристики, які були запропоновані, включають цілісність, точність, чіткість, ясність, глибину, здатність охопити велику кількість аспектів, логіку, значущість і актуальність [11, с.7]. Офісом директора національної розвідки США було розроблено перелік аналітичних компетенцій, який включає [12]:

- об'єктивність
- незалежність політичних міркувань та позицій
- своєчасність
- відповідні стандарти розвідувальної діяльності, розроблені з урахуванням специфіки всіх джерел, які визначають, що аналітичний продукт повністю:
  - ✓ *описує якість та надійність базових джерел*
  - ✓ *представляє всі застереження та сумніви/впевненість у аналітичних судженнях;*
  - ✓ *розрізняє фундаментальні оперативні дані та припущення/судження аналітиків*
  - ✓ *дає можливість застосувати альтернативний аналіз за необхідності*
  - ✓ *демонструє відповідність продукту принципам та вимогам політики національної безпеки США*
  - ✓ *використовує логічну аргументацію;*
  - ✓ *демонструє послідовність аналізу з плином часу або висвітлює зміни та роз'яснює відповідні умови і обґрунтування*
  - ✓ *подає точні судження та оцінки.*

Логічні процеси мислення

Здатність мислити логічно, прослідковувати тенденції і прогнозувати можливе майбутнє є критичною для аналітика. І навпаки - ті, хто не може структурувати дані і відфільтрувати з них матеріал для аналізу, не досягнуть успіху. Логічне мислення можна розвивати, хоча дехто ці навички опановує швидше – для цього можна використовувати різноманітні головоломки та запропоновані у спеціальній літературі вправи або ж з використанням складніших інтелектуальних технік. Логічна аргументація є ключовим елементом не тільки аналізу, а й процесу формування грамотного усного і писемного мовлення [13].

Критичне мислення

Критичне мислення є по суті, обдумуванням прочитаного, написаного чи сказаного [11]. У багатьох випадках люди виконують свою роботу без такого обдумування, тобто застосовують один і той самий підхід до вирішення різних проблем, а потім задаються питанням, чому проблеми не вирішені.

Годфрі і Харріс визначають процес розвідки як «часом суто матеріальний, та в будь-якому випадку інтелектуальний» [14, с.2]. Малося на увазі те, що когнітивні процеси завжди повинні застосовуватися під час опрацювання даних, незалежно від того, чи були ці дані відправлені за межі агенції або вилучені, чи вони протягом всього часу були «під рукою». Під критичним мисленням, яке так часто згадується, ми розуміємо в першу чергу саме процес обдумування.

Застосування критичного мислення в окремій ситуації змушує дивитися на проблему з інших точок зору. Також можуть існувати інші можливі пояснення. Інтерпретація даних без врахування всіх можливостей може призвести до неточного аналізу, який, у свою чергу, може бути фатальною помилкою.

Навички комунікації

Здатність спілкуватися письмово або усно є ключем до створення зрозумілих споживачеві аналітичних продуктів. Оперативні дані нічого не вартують, якщо ними не діляться з іншими. Можна легко пояснити обставини будь-якої заплутаної справи тим, хто має до її розслідування прямий стосунок; аналітики повинні вміти пояснити це просто доступно тим, хто отримує інформацію вперше.

Ефективна письмова комунікація - це 65% якісної організації і 35% концентрованого та чіткого викладу. Аналітики зобов'язані читати та асимілювати дані з різних джерел, підсумовуючи їх за необхідності - це частина їхньої рутинної діяльності. Те ж саме стосується і усних брифінгів, хоча і в цьому випадку необхідні навички оформлення презентацій.

Характеристики аналітика

Навички автономної роботи - аналітики повинні мати можливість працювати самостійно без постійного нагляду. Вони повинні вміти мотивувати себе і самостійно визначати свої пріоритети, тобто, ідентифікувати проблему і обирати спосіб її вирішення. Це є особливо актуальним для менших департаментів, де керівники не мають досвіду координації аналітичної діяльності. У цих випадках аналітик повинен виконувати роботу максимально ефективно та отримати статус «незамінного» фахівця.

Гнучкість - аналітики повинні мати можливість пристосовуватися до змін. Досить часто саме ці люди займають позиції на «лінії фронту», виконуючи надскладні завдання, які вимагають найсучаснішого устаткування та методик – саме тому вони повинні бути в змозі пристосуватися до зовнішніх змін, виконуючи при цьому роль каталізаторів вказаних перетворень.

Наполегливість - аналітики повинні бути наполегливими у своїй роботі, під час опрацювання слідів та «зачіпок» і водночас виступати агентами змін. У кримінальному світі злочинці розраховують на те, що правоохоронці «зійдуть з дистанції» і відмовляться від подальших спроб. Наполегливість - це те, що дозволяє нам досягати цілей, коли вони здаються недосяжними.

Готовність представляти судження - аналітики повинні вміти «відстоювати» подані власноруч висновки як фахівці, які докладали максимум зусиль для дослідження та опрацювання даних. Хоча раніше коментарі аналітиків фактично обмежували і зводили до рівня фактичної звітності, сьогодні менеджери потребують більш конструктивного внеску від аналітичного компоненту під час прийняття рішень. Нездатність (або небажання) дійти певного висновку щодо даних не має відповідного позитивного ефекту як для аналітиків, так і для всієї правоохоронної структури.

Аналітики розробили стандарти та критерії, за якими можливо оцінити їхню роботу з залученням професійних організацій. Годфрі висловив припущення, що існують два типи аналітиків: неспеціалісти та спеціалісти. Ці аналітики повинні були бути високоосвіченими людьми з енциклопедичними знаннями, і прагнути вивчати нові сфери – саме вони «досить швидко зробили неоціненний внесок у розвиток системи кримінального аналізу» [15, с.42]. З іншого боку, аналітики-спеціалісти можуть надавати свої послуги на контрактній основі (сумісники) чи залучатися як працівники інших структур для участі у визначених розслідуваннях.

Наразі керівництво правоохоронних органів усвідомлює, що аналітики-спеціалісти можуть бути підготовлені шляхом поєднання теоретичного компоненту з можливістю «відшліфовувати» практичний досвід на займаних в правоохоронних структурах посадах. Наприклад, особа з дипломом магістра за спеціальностями «Бізнес» чи «Бухгалтерський облік» може бути найнята для проведення фінансового аналізу, якщо це вважається за доцільне, а потім отримати додаткову підготовку щодо специфічних аналітичних аспектів (судова бухгалтерія). Аналітики з дипломами фахівців ІТ-галузі (повна вища освіта чи курси підвищення кваліфікації) можуть бути залучені до роботи, пов'язаної з запуском та вдосконаленням баз даних. Випускники філологічних та лінгвістичних факультетів

користуються популярністю у відділах боротьби з незаконним розповсюдженням наркотиків та запрошуються до участі в міжнародних операціях.

НАВЧАННЯ

Сьогодні більшість агенцій встановлює в якості обов'язкової вимоги наявність базової вищої освіти (чотирирічний термін) для аналітиків-початківців; деякі встановлюють аналогічну вимогу і для працівників поліції. IALEIA вимагає завершення дво- або чотирирічного курсу для сертифікації, залежно від її рівня. Можна сподіватися, що аналітик, який завершив дворічний курс підготовки і має сертифікат, який необхідно регулярно підтверджувати, виявлятиме бажання підвищувати свою кваліфікацію та проходити чотирирічний курс перед поданням заявки на отримання відповідного сертифіката.

Загальний план для працівників підрозділів, залучених до боротьби з наркотрафіком, опублікований Центром контролю за обігом наркотиків у США, визначає, що аналітики повинні мати дипломи про завершення чотирирічних курсів [15, с.42]. У декількох країнах розробляються спеціальні програми підготовки у сфері аналітики для здобувачів ОКР «Бакалавр» і «Магістр». Деякі магістерські програми не визначають обов'язковим наявність диплому про завершення чотирирічного курсу, але передбачають можливість врахування наявного практичного досвіду роботи у конкретних сферах замість свідоцтв про здобуття певної кваліфікації.

У 2004 році IALEIA представила набір аналітичних стандартів, розроблений спільно з Глобальною робочою групою з питань розвідувальної діяльності. Ці стандарти для аналітиків розглядаються нижче.

Початкова підготовка аналітиків повинна включати мінімум 40 годин із залученням інструкторів та викладачів з досвідом здійснення аналітичної діяльності в правоохоронних структурах. Підготовка повинна включати, але не обмежуватися наступними темами [17, с.6-7]:

- Цикл / процес аналізу
- Правоохоронна діяльність, керована аналітичною розвідкою (Intelligence-led Policing)
- Опрацювання матеріалів
- Оцінка інформації
- Критичне мислення
- Логіка
- Розробка висновків та рекомендацій
- Плани збору
- Методи і джерела досліджень
- Аналіз злочинних патернів
- Аналіз зв'язків / мереж
- Аналіз телефонних переговорів / комунікації
- Аналіз потоків
- Просторовий / географічний аналіз
- Фінансовий аналіз
- Стратегічний аналіз
- Аналітичний виклад (підготовка документів)
- Навички презентування
- Статистика
- Графічні методи
- Комп'ютеризовані програми для підтримки аналізу
- Етика
- Професіоналізм

Післядипломна освіта – аналітики повинні проходити додаткові навчальні курси (тривалістю мінімум вісім годин на рік) у форматі, що об'єднує теоретичний блок, семінарські заняття, дистанційне навчання та самостійну підготовку. Організатори таких курсів повинні мати відповідний практичний чи науковий досвід. Курси можуть також включати теми, представлені у попередньому переліку стандартів [16, с.10].

Професійний розвиток - аналітики повинні вдосконалювати наявні знання та навички протягом всієї своєї кар'єри і отримувати відповідну підтримку з боку роботодавців - це однозначно позитивно відобразиться на результатах розвідувальної роботи, незалежно від того, хто саме виконує ці функції.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Литвинов В.А., Козловська Т.А., Жерновий М.М., Овсянюк Д.І. Історія становлення підрозділів кримінального аналізу Національної поліції України. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України*: матеріали міжвідом. наук.-практ. конф. (Київ, 11 серп. 2022 р.). Київ: НАВС, 2022. С. 113-116.

2. Шинкаренко І.Р. Проблеми запровадження кримінального аналізу в діяльність підрозділів кримінальної поліції: теоретико-історичне підґрунтя. *Науковий вісник ДДУВС*. 2017. № 1. С. 233-242.
3. Овсянюк Д.І. Актуальні питання правового та патріотичного виховання здобувачів вищої освіти ЗВО зі специфічними умовами навчання в умовах воєнного стану. *Кримінальний аналіз як сучасний інструмент підвищення ефективності протидії злочинності*: матеріали наук.-теорет. конф. (Київ, 19 трав. 2022 р.). Київ: НАВС, 2022. С. 105-107.
4. Carter, D.L., (1990). *Law Enforcement Intelligence Operations: Concepts, Issues, Terms*. Michigan: Michigan State University Press.
5. Colwill, J., & Birchall, G., (1992). *Practical Management: An Introduction to Management Skills*. Melbourne, Longman.
6. Cromwell, Robert (October 1998). Analyst's Core Competencies. *Presentation at IALEIA Conference*.
7. Martens, F.T. (1990). The Intelligence Function. In Andrews, P.P. & Peterson, M.B. (eds). *Criminal Intelligence Analysis*. Loomis, Ca: Palmer Enterprises.
8. Makridakis, S.G. (1990). *Forecasting, Planning and Strategy for the 21s' Century*. New York, MacMillan.
9. Nankervis, A., Compton, R. & McCarthy, T. (1996). *Strategic Human Resources Management*. 2nd ed. Melbourne: Nelson.
10. *International Association of Law Enforcement Intelligence Analysts* (1997). Guidelines for Starting an Analytic Unit. Lawrenceville, NJ: IALEIA.
11. Paul, Richard & Linda, Elder (2006). *A Miniature Guide to Analytic Thinking*. Berkeley, CA: The Critical Thinking Foundation.
12. Office of the Director of National Intelligence (2007). Intelligence Community Directive 203. Washington, DC: Office of the Director of National Intelligence (June 21).
13. Govier, Trudy (2005). *A Practical Study of Argument Sixth Edition*. Belmont, CA: Thompson Wadsworth.
14. Godfrey, E. Drexel & Don R., Harris (1976). *The Basic Elements of Intelligence*. Washington, DC: Law Enforcement Assistance Administration.
15. Harris, Don R. (1976). *The Basic Elements of Intelligence*. 2nd Edition. Washington, DC: Law Enforcement Assistance Administration.
16. International Association of Law Enforcement Intelligence Analysts (2004). L*aw Enforcement Analytic Standards*. Richmond, VA: International Association of Law Enforcement Intelligence Analysts and Global Justice Information Sharing Initiative.

DOI: https://doi.org/10.36486/978-966-2310-66-5-11

Кожна зі сторін вважає, що вона має рацію, а опонент помиляється. Насправді обидві сторони мають рацію в рамках власної парадигми.

Джоел Баркер

РОЗДІЛ 11
Термінологія та сутність кримінального аналізу

Олександр Користін
Владислав Бурангулов

Сучасний етап розвитку правоохоронної практики, з-поміж іншого, характеризується активним упровадженням та розвитком кримінального аналізу, забезпечуючи повноту та ефективність його використання на фоні потреби інноваційного розвитку інформаційно-аналітичної функції. Водночас теоретичне осмислення кримінального аналізу, як нового інституту правоохоронної діяльності з відповідною термінологією, сприйняттям його змісту, форм та видів, процесу та формування аналітичного продукту, потребує активного залучення вітчизняної наукової спільноти.

Наразі кримінальний аналіз, з точки зору методології застосування, що базується на досягненнях світової науки та практики, є достатньо визначеним інститутом й у своїй основі не має принципових відмінностей інституціонального упровадження різними суб'єктами в межах однієї юрисдикції. Але вітчизняна практика все ж вказує на низку проблемних питань щодо узгодженості сприйняття змісту, видів, рівнів кримінального аналізу і щодо комплексності та системності його упровадження різними правоохоронними органами.

Частково ця проблема пов'язується з відсутністю достатнього наукового аналізу цього сегменту новизни, що має коріння іншомовного походження та часто на практиці використовується без належного обґрунтування і нерідко хибно трактується.

> *Використання кримінального аналізу в практиці вітчизняної правоохоронної діяльності нерідко йде у розріз з його сутністю, яка формувалася десятиліттями відповідною зарубіжною практикою та наукою,*

і сьогодні потребує принципового теоретичного осмислення змісту, розпочинаючи з самого терміна «кримінальний аналіз».

Наразі мають місце дві особливості, на які потрібно звернути увагу перш ніж продовжувати аналіз змісту терміна «*кримінальний аналіз*». Одна з них це те, що нормативне закріплення терміна «кримінальний аналіз» і саме на рівні закону в Україні реалізовано лише у 2021 році у зв'язку з прийняттям Закону України «Про бюро економічної безпеки України» [1], але практичне його застосування сягає ще 2006-2008 років, з упровадженням його у діяльності Державної прикордонної служби України [2; 3], і друге – сам термін запозичено з англомовного використання «*crime analysis*».

Враховуючи запозиченість зазначеного терміна з іншої мови зазначимо, що семантика запозичених слів досить часто не збігається із семантикою їх прототипів у мові-джерелі. Виділяють різні типи семантичних змін запозиченої лексеми, зокрема: спрощення семантичної структури (запозичення в одному чи кількох значеннях за його значно ширшої полісемії в мові-джерелі); ускладнення семантичної структури (поява нових значень на ґрунті мови-реципієнта, в тому числі й таких, яких запозичене слово не мало в мові-джерелі); звуження значення запозиченого слова внаслідок його спеціалізації; розширення, зумовлене генералізацією відповідного поняття; зміна значення (термін уживається в системі мови-реципієнта в значенні, якого немає відповідне слово в мові-джерелі) [4, с. 153-154]. Тобто обґрунтованим є зауваження того, що, не завжди прямий переклад професійного терміна є достатнім та об'єктивним щодо змісту сприйняття чи контексту застосування. Термінологічне закріплення іншомовного виразу є процесом обґрунтованої інтерпретації із врахуванням мови, культури, традицій і, звісно, змістовного наповнення.

Водночас використання англомовного терміна «crime analysis» в інтерпретації «кримінальний аналіз», певним чином пов'язується з тим, що 3 травня 2006 р. за ініціативою Представництва Міжнародної організації з міграції в Україні проведено переговори представників Посольства США

в Україні, Міжнародної організації з міграції, Адміністрації Держприкордонслужби України та Головної комендатури Прикордонної варти Республіки Польща, результатом яких стали досягнуті домовленості про запровадження спільного проекту щодо надання допомоги Державній прикордонній службі України з опрацювання підходів до запровадження системи управління ризиками та кримінального аналізу. Тобто

> *«До правоохоронних органів України метод кримінального аналізу прийшов з Республіки Польща. Одним із перших прикордонних відомств, які успішно започаткували цю систему, є Прикордонна варта Республіки Польща» [5].*

Таким чином, вивчаючи засади кримінального аналізу на базі польської правоохоронної системи, було запозичено інтерпретацію терміна саме з польської практики застосування – «*analizy kryminalnej*», «*analiza kryminalna*», який українською перекладається прямо – «кримінальний аналіз». Водночас термін англійською «*crime analysis*», що використовується в англомовних країнах і, перш за все, у Великій Британії та США (де він виник й існує до сьогодні як окремий інститут) у прямому перекладі передбачає інтерпретацію – *аналіз злочину (злочинності)*.

> *Саме на це вказує історичний аналіз виникнення й поширення кримінального аналізу в правоохоронному середовищі та сприйняття в інтерпретації українською мовою як якісний аналіз злочину та подальше порівняння його з аналогічними минулими подіями.*

Водночас елементарною номінативною одиницею професійно-орієнтованих підмов вважається *термін* (від лат. *terminus* – межа, кордон) [6]. У ракурсі сучасного лінгвокогнітивного підходу термін уособлює особливу когнітивно-інформаційну структуру, у якій акумулюється виражене в конкретній мовній формі професійно-наукове знання [7, с. 332]. У зв'язку з цим терміни та їхні сукупності – *терміносистеми* й *термінополя,* розглядаються в тісному зв'язку з концептами як результатами мовленнєво-мисленнєвої діяльності [8]. Різниця між терміном і словом об'єктивно зумовлена тим, що вони відображають явища різних рівнів мисленнєвої діяльності – наукове мислення і побутове оперування уявленнями [7, с. 332].

Таким чином, юридичний термін є словом або словосполученням, яке уніфіковано вживається у сфері правових відносин, позначає юридичне поняття з певним ступенем дефінітивності, заданою моносемічністю (тобто однозначністю, семантичною визначеністю) та функційною стійкістю [9].

Наразі, фактично, саме

> *технічне перенесення з польської практики правоохоронної діяльності терміна «analizy kryminalnej», що дійсно використовувався у польських нормативних актах й правоохоронній практиці, та його інтерпретація українською як «кримінальний аналіз», а не «аналіз злочинності», і стало причиною застосування в українській правоохоронній практиці та нормативних актах терміна «кримінальний аналіз.*

Таке перенесення характеризується окремим і відомим серед мовників типом спеціальних лексичних одиниць: *професіоналізмом* – ненормованою спеціальною лексикою, обмеженою вживанням в усному мовленні професіоналів [10, с. 332].

Водночас оскільки «crime analysis» є англомовним терміном, ключовим все ж залишається його переклад українською та подальше змістовне наповнення і, що важливо, суспільне сприйняття та професійне використання різноманітних похідних інтерпретацій, які сьогодні набувають все більш масового вживання і не тільки у професійній сфері, зокрема, «кримінальна аналітика», «центр кримінальної аналітики», «кримінальний аналітик» тощо.

Семантичне освоєння запозиченого слова насамперед передбачає становлення його лексичного значення на ґрунті мови-реципієнта [9]. Аналізуючи семантику терміна-словосполуки «кримінальний аналіз» зазначимо, що у ньому використовується опорне слово «аналіз» та прикметникове означення «кримінальний».

Доречним є, перш за все, зупинитися на самому слові «аналіз», яке ми за звичай сприймаємо як розкладання певного складного явища на більш прості складові чи елементи. Зокрема, найдоступніші джерела (Вікіпедія) розкривають зміст терміна «аналіз» (від грец. Αναλυσις – «розклад») – розчленування предмета пізнання, абстрагування його окремих сторін чи аспектів. Водночас це метод дослідження, який вивчає предмет, уявно чи реально розчленовуючи його на складові елементи, як-от: частини об'єкта, його ознаки, властивості, відношення відтак розглядає кожен з виділених елементів окремо в межах єдиного цілого [10].

Наразі наукова література достатньо часто викладає думки вчених щодо терміна «аналіз». Зокрема звертає на себе увагу вислів відомого англійського філософа ще на початку XX сторіччя Бертрана Рассела у праці «Принципи математики»: *у сфері інтерпретацій мови філософських теорій рішення*

– це аналітичний метод, який передбачає дроблення тексту до тієї межі, поки теорія не виявиться або як набір осмислених тверджень, або як повна нісенітниця. Рассел вважав, що за такого підходу більшість філософських «проблем» взагалі перестають існувати. Його визначення змінили традиційні англійські підходи до філософії: «аналітичний підхід» став єдиним потужним методом [11].

Важливим для нашого дослідження є саме це визначення, бо акцентує увагу на аналітиці, на аналітичному підході у визначенні змісту «аналізу», а відтак і «кримінального аналізу».

Відомості про першу згадку слова «кримінальний» (XVII ст.) та його фіксація в сучасних тлумачних словниках української мови засвідчують, що в семантичній структурі цього слова є етимологічно виявлені домінантні семи (елементарні ознаки змісту) «злочинний / злочин / злочинність / злочинець» і «карний / кара / покарання» та власне диференційні ознаки «судовий / осуд», «неприпустимий», «розслідування». Тобто в українській мові слово кримінальний відноситься до синонімічного ряду «кримінальний – карний – злочинний» і саме у такій послідовності [12], що, власне, й спричиняє небажані для терміна «кримінальний» різночитання.

Наразі прикметник «кримінальний» запозичено з латини багато сторіч тому: латинський прикметник *criminalis* походить від іменника *crimen (criminis)*, що означає злочин. Відповідно в сучасній літературній мові він набув таких значень: 1) злочинний; 2) той, що стосується вивчення злочинів і злочинності, боротьби і запобігання злочинам [13, с. 370].

Таким чином, дійсно має місце різночитання терміна «кримінальний аналіз» і особливо похідних від нього родових виразів: «кримінальна аналітика», «центр кримінальної аналітики», «кримінальний аналітик» тощо. Водночас, враховуючи факт досить тривалого (з 2006 року) практичного термінологічного застосування у професійному середовищі українських правоохоронних органів, малоймовірним є сприйняття терміна «кримінальний аналіз» як «злочинний аналіз».

Водночас залишається нав'язливою думка щодо неоднозначного семантичного сприйняття термінів:

«кримінальний аналітик» – *злочинець чи той хто протидіє злочинності?*;

«кримінальна аналітика» – *злочинна аналітика, чи діяльність з аналізу злочинності?*

Це дійсно є дискусійним, але

> *з точки зору правозастосування та однозначності у визначеннях та сприйнятті як у професійному середовищі, так і назагал у суспільстві, важливим є обґрунтоване їх використання з прямим означенням змісту, уникаючи різночитань та семантичного сприйняття.*

Право, як і будь-яка інша галузь знань, вербалізується мовними засобами, надбудованими над загальновживаною мовою. Термінологія права, яку також називають термінологією правозастосовної практики, є формалізованим утворенням для семіотичного забезпечення професійного спілкування, а вербальні продукти такого спілкування втілюють частину правової картини світу відповідної лінгвокультури [7, с. 332].

> *Тобто термінологія правозастосовної практики має бути основою професійної культури та відображати узгоджене професійне використання й застосування з семантичним сприйняттям у суспільстві.*

Прикладом узгодженого застосування є діяльність Міжнародної асоціації аналітиків злочинності (International Association of Crime Analysts – IACA). Незважаючи на те, що у назві IACA використовується словосполучення «Crime Analysts», що українською теж має дискусійну інтерпретацію, все ж, активно займаючись сертифікованою підготовкою аналітиків, у назві тренінгових програм використовують словосполучення «Law Enforcement Analyst» [14], яке не викликає неоднозначності семантичного сприйняття і прямо інтерпретується як «аналітик правоохоронного органу».

І такий підхід є чітким прикладом того, як необхідно уникати різночитань у використанні юридичних термінів.

Таким чином, *враховуючи певні особливості професійного використання терміна «кримінальний аналіз», можливим та достатньо обґрунтованим є сприйняття та узгоджене використання його в інтерпретації як «аналіз злочинності».*

> *Водночас некоректним все ж залишається професійне використання термінів «кримінальний аналітик», «кримінальна аналітика».*

Уникаючи різночитань та неадекватного сприйняття їх змісту, порівняно з професійним осередком, більш широкою громадянською спільнотою, використання термінів:

> *«аналітик правоохоронного органу»,*
> *«аналітик злочинності»,*
> *«аналітична діяльність, що пов'язана з дослідженням злочинності»,*
> *«аналітика злочинності» –*

відповідно, є більш коректним та менш дискусійним у визначенні відповідної правоохоронної діяльності.

З'ясувавши семантику терміна «кримінальний аналіз», важливим є подальше формулювання відповідної дефініції. У правоохоронній діяльності існує безліч визначень кримінального аналізу.

Відомий фахівець у зазначеній сфері професорка Редфордського університету Рейчел Боба Сантос (*Rachel Boba Santos*) зазначає [15], що кримінальний аналіз – це термін, який використовується для опису широкого кола дій та ідей. З потенційно більшої цінності це термін проблемного аналізу. Проблемний аналіз випливає з концепції Германа Гольдштейна щодо проблемно орієнтованої моделі поліцейської діяльності (*problem-oriented policing*) (1990 р.) і означає форму кримінального аналізу, що *здійснюється в межах поліцейської агенції, на основі формальної теорії кримінального правосуддя, методів дослідження, а систематизація даних та процедури аналізу використовуються для проведення поглибленого вивчення проблем злочинності та їх оцінювання.*

Інший вчений Майкл Скот (*Michael S. Scott*) також зазначає [16], що *кримінальний аналіз тісно пов'язаний з організацією проблемно-орієнтованої поліцейської діяльності, процесу, який не лише зосереджується на виявленні та вирішенні проблем злочинності, але також є більш комплексною основою для покращення реагування поліції на всі аспекти її роботи.*

Вирішення проблем – це процес мислення, за допомогою якого працівники, зокрема, аналітики досягають своїх цілей, і часто вирішується через процес SARA (*Scanning, Analysis, Response and Assessment*): сканування, аналіз, відповідь і оцінювання [17].

Наразі за останні десятиріччя багато вчених розробляли визначення кримінального аналізу.

Такі автори як Еміг (*Emig*), Хек (*Heck*), та Кравіц (Kravitz) [18] зазначають, що *кримінальний аналіз стосується набору систематичних аналітичних процесів, які надають своєчасну доречну інформацію про моделі злочинності та кореляції тенденцій злочинності.*

Це насамперед тактичний інструмент. Звіти патрулів і записи злочинів містять дані про місця злочину, зброю, способи дії, викрадені транспортні засоби та підозрюваних. Аналіз та порівняння даних у досьє з поточними справами може дати патрульним поліцейським важливу інформацію про діяльність у їхніх районах. Це включає розробку моделей злочинів, опис викраденого майна та ідентифікацію підозрюваних. Використовуючи цю інформацію, патрулі можуть краще використовувати ресурси.

Водночас Готліб (*Steven Gottlieb*), Аренберг (*Sheldon Arenberg*) та Сінх (*Raj Singh*) у своїй книзі [19, с. 13] вказують на те, що кримінальний аналіз – *це набір систематичних аналітичних процесів, спрямованих на надання своєчасної та відповідної інформації щодо моделей злочинності та кореляцій тенденцій для допомоги оперативному та адміністративному персоналу в плануванні використання ресурсів для запобігання та припинення злочинної діяльності, сприяння процесу розслідування, збільшення затримань і розкриття справ.*

У цьому контексті кримінальний аналіз підтримує низку функцій: розгортання патрулів, спеціальні операції та тактичні підрозділи, розслідування, планування та дослідження, запобігання злочинності та адміністративні послуги (бюджетування та планування програм).

А Веллані (*Vellani*) та Нахун (*Nahoun*) взагалі максимально узагальнено підійшли до цього питання, зазначаючи [20, с. 8], що *кримінальний аналіз – це дисципліна, орієнтована на деталі, у якій аналітик намагається знайти правду щодо цієї ситуації, використовуючи методи та правильну інформацію для підтвердження правди, щоб можна було сформулювати ефективний план.*

Хоча ці визначення відрізняються за специфікою, у них є кілька спільних компонентів: усі погоджуються, що

> *кримінальний аналіз підтримує місію поліцейського відомства, використовує систематичні методи й інформацію та надає інформацію широкому колу аудиторій.*

Саме виходячи з такого узагальнення професорка Рейчел Боба Сантос (*Rachel Boba*) резюмуючи, подає ці елементи у більш простій формі та зазначає, що кримінальний аналіз по суті є

> *«систематичним вивченням проблем злочинності та правопорушень, а також інших питань, пов'язаних з правоохоронною діяльністю, включаючи соціально-демографічні, просторові та часові чинники, з метою допомоги у затриманні злочинців, об'єктивного сприйняття інформації про злочинне середовище, оцінювання та зниження рівня злочинності, запобігання окремим видам злочинів» [21].*

Розкриваючи більш широко дефініцію, професорка Рейчел Боба зазначає, що *кримінальний аналіз не є випадковим чи анекдотичним, а передбачає застосування процедур збору даних з використанням соціальних наук, аналітичних і статистичних методів [21].*

Кримінальний аналіз використовує як якісні, так і кількісні дані та методи, залежно від аналітичної та практичної потреби. Аналітики використовують якісні методи, коли досліджують нечислові дані з метою виявлення основних значень і моделей взаємозв'язків. Якісні методи, характерні для кримінального аналізу, включають польові дослідження (наприклад, спостереження за характеристиками місцевості) й аналіз контенту (наприклад, вивчення викладеного в поліцейських звітах). Зокрема, наративи звітів про злочини вважаються якісними даними, оскільки велику кількість наративів майже неможливо статистично проаналізувати, і вони в першу чергу досліджуються для визначення загальних тем і закономірностей. Аналітики використовують кількісні дані та методи, коли проводять статистичний аналіз числових або категорійних даних. Така інформація, як дата, час, місце та тип злочину, є кількісною, оскільки статистику можна використовувати для аналізу цих змінних. Хоча велика частина роботи з аналізу злочинності є кількісною, аналітики використовують прості статистичні методи, такі як частоти, відсотки, середні значення та показники.

Центральним фокусом кримінального аналізу є вивчення злочинності та правопорушень. Вивчення (дослідження) – це систематичний спосіб перегляду інформації про злочини та правоохоронну діяльність. Таким чином,

> *кримінальний аналіз полягає не у випадковому дослідженні інформації, а в застосуванні формальних аналітичних і статистичних методів, а також методології дослідження до інформації правоохоронних органів відповідно до правил соціальних наук.*

Центром уваги правоохоронних органів є злочини, як ті, про які повідомлено, так і ті, про які не повідомлено. Таким чином, основним типом даних, які аналізуються, є злочини та інформація, що їх оточує, зокрема арешти, правопорушники, жертви, майно та докази.

Окрім протидії злочинності, правоохоронні органи займаються багатьма іншими проблемами й таким чином збирають багато інших типів даних. Прикладами таких правоохоронних органів, які часто доступні для аналітиків, є звернення до органу (наприклад, скарги на шум, повідомлення про крадіжку, певні підозрілі дії), інформація, пов'язана з характером інцидентів, правопорушниками та жертвами чи об'єктами злочину (цілями є неживі предмети, наприклад, будівлі чи майно), про дорожній рух (наприклад, аварії та ситуації), сприйняття та відчуття громадянами (наприклад, страх перед злочинами, задоволеність діяльністю поліції), віктимізація, записи про пробацію та інформація про умовно-дострокове звільнення тощо. Аналітики також вивчають інші питання, пов'язані з діяльністю поліції, такі як потреби в персоналі та напрями службової діяльності тощо. Незважаючи на те, що ця дисципліна називається кримінальним аналізом, вона насправді включає набагато більше, ніж просто дослідження злочинів (злочинності).

Пов'язуючи правоохоронну діяльність із соціально-демографічними, просторовими та часовими чинниками, кримінальний аналіз не залишається осторонь щодо виявлення закономірностей і вивчення зв'язків даних про злочини. Незважаючи на те, що багато різних характеристик злочинності та правопорушень є актуальними для аналізу злочинності, зазначені три види інформації є найважливішими у діяльності аналітиків, які досліджують злочинність.

Соціально-демографічна інформація *стосується особистих характеристик окремих осіб і груп, таких як стать, раса, дохід, вік, освіта тощо*. На індивідуальному (мікро) рівні соціально-демографічна інформація використовується для розшуку та ідентифікації підозрюваних у вчиненні злочинів. На макрорівні соціально-демографічна інформація використовується для визначення характеристик груп і їхнього відношення до злочинності. Наприклад, інформація може бути використана для відповіді на запитання: «Чи є людина чоловічої статі, віком 30-35 років, з каштановим волоссям і карими очима, підозрюваним у причетності до конкретного пограбування?» або «Чи можуть демографічні характеристики пояснити, чому в одному районі рівень злочинності вищий, ніж в іншому?»

Просторова характеристика *є центральною для розуміння природи проблеми.* Місце вчинення злочину чи діяльності, і зв'язок цих місць одне з одним та з іншою інформацією є важливим фактором аналізу злочинності. Важливе не лише з'ясування місця вчинення злочину, але й характеристики тих місць і середовища, в яких відбувається злочин. Таким чином, дослідження просторових даних, таких як мережа вулиць, інформація про земельні ділянки, фотографії, розташування шкіл,

зонування підприємств і житлових будинків, серед іншого, є обов'язковим для ефективного аналізу злочинності. Сучасні можливості на основі удосконалення комп'ютерних технологій і доступності електронних даних сприяли більшій ролі просторового аналізу в кримінальному аналізі. Візуальне відображення місць злочину та їхнього зв'язку з іншими подіями та географічними об'єктами має важливе значення для нашого розуміння природи злочину та правопорушення. Сучасні розробки в кримінологічній теорії спонукали аналітиків зосередитися на географічних моделях злочинності, досліджуючи ситуації, в яких жертви та правопорушники поєднуються в часі та просторі.

***Часові чинники** злочинності, правопорушень та інших питань, пов'язаних з правоохоронною діяльністю, є також важливим компонентом кримінального аналізу*. Аналітики проводять кілька рівнів часового зрізу, включаючи вивчення довгострокових моделей і тенденцій злочинності протягом кількох років, сезонного характеру злочинності та моделей за місяцями; дослідження моделей середньої тривалості, таких як моделі за днями тижня та часом доби; та дослідження короткострокових закономірностей, таких як закономірності за днями тижня, часом доби або проміжком часу між інцидентами в рамках певної серії злочинів.

Заключна частина наведеного професоркою Рейчел Боба визначення – «*допомога у затриманні злочинців, об'єктивному сприйнятті інформації про злочинне середовище, оцінюванні та зниженні рівня злочинності, запобігання окремим видам злочинів*» – загалом ***вказує на 4 цілі кримінального аналізу**:*

***1 ціль** – основною функцією кримінального аналізу є підтримка діяльності правоохоронних органів.* Одним з першочергових завдань правоохоронних органів є затримання злочинців; отже, однією з основних цілей кримінального аналізу є допомога в затриманні злочинців. Наприклад, детектив може розслідувати інцидент пограбування, під час якого злочинець використав певний спосіб вчинення злочину. Аналітик може допомогти детективу, ідентифікуючи попередні пограбування за аналогічним способом. Крім того, аналітик може проводити аналіз інцидентів крадіжок за часом доби/дня тижня, що допоможе скоординувати поліцейські заходи з розшуку та затримання злочинця.

***2 ціль** – запобігання злочинності й саме у спосіб відмінний від затримання*. Реалізація цієї мети є саме специфічною функцією кримінального аналізу. Наприклад, працівники поліції проводять профілактичні заходи з метою запобігання квартирним крадіжкам, максимально ефективно спрямувавши свої можливості та ресурси. Аналітики, надаючи просторовий аналіз квартирних крадіжок, аналіз того, як, коли та де сталися крадіжки, а також аналіз того, які речі були вкрадені, звужують коло поліцейських заходів, вказують на конкретні громади та території підвищених ризиків й необхідності посилення патрулювання.

***3 ціль** – злочинність є перш за все соціально-економічною проблемою*. Багато проблем, з якими має справу поліція або які потребують вирішення, не є кримінальними за своєю суттю; скоріше, вони більше пов'язані з якістю життя та порушенням громадського порядку, зокрема: скарги на гучний шум, контроль дорожнього руху та сусідські суперечки тощо. Таким чином, забезпечення громадського порядку є безпосередньою метою діяльності поліції, а відтак і метою діяльності підрозділів кримінального аналізу. Аналітики здійснюють дослідження та аналіз проблем у сфері громадського порядку, визначають та аналізують стан за певними індикаторами щодо порушень правил поведінки в громадських місцях, дорожньо-транспортних пригод, проведення профілактичних заходів тощо з метою забезпечення підрозділів поліції необхідною інформацією для впливу на правопорушення, вирішення проблем, що їх супроводжують, перш ніж вони стануть серйознішими кримінальними проблемами.

***4 ціль** – остаточною метою кримінального аналізу є допомога в оцінці зусиль поліції*. Таке оцінювання стосується двох основних сфер: рівня успіху програм та ініціатив, запроваджених для контролю та запобігання злочинності й правопорушенням громадського порядку, а також ефективності управління поліцейськими органами та підрозділами. Останніми роками місцеві поліцейські підрозділи все більше зацікавлені у визначенні ефективності різноманітних програм та ініціатив з контролю та запобігання злочинності. І аналітики допомагають поліцейським департаментам в оцінці внутрішніх організаційних процедур, таких як розподіл ресурсів, зміна географічних кордонів, прогнозування потреб у персоналі та розробка показників ефективності. Такого роду контроль потребує постійної уваги для забезпечення ефективності поліцейських заходів, діяльності як окремих працівників поліції, так і підрозділів загалом.

Важливі акценти зроблено у виданні 2017 року Міжнародної асоціації аналітиків злочинності (*IACA*) [22] та зазначено, що для стороннього спостерігача «кримінальний аналіз» є досить загальним терміном, який може охоплювати багато процесів у поліцейській діяльності та кримінології, виділяючи водночас особливості того, що не є кримінальним аналізом.

І дійсно, в Україні сьогодні мають місце непоодинокі думки різного рівня фахівців і наприкінці жаль вчених, які кримінальний аналіз відносять і до кримінології, і до криміналістики тощо, називаючи його кримінологічним аналізом та криміналістичним аналізом. Але ми зауважимо таке,

базуючись на твердженнях та дослідженнях в авторитетних виданнях та знаних фахівців саме у цій сфері.

Кримінальний аналіз – це не розслідування на місці злочину чи криміналістика.

Кримінальний аналіз – це аналіз даних, включаючи розвідувальний аналіз, але не аналіз доказів. Аналітики підрозділів кримінального аналізу не реагують на місця злочину, не збирають відбитки пальців, не вивчають бризки крові та не аналізують ДНК. Цю важливу роботу виконують підрозділи, що розслідують злочини.

Кримінальний аналіз – це не психологічне профілювання.

Хоча і мають місце певні елементи психологічного профілювання за окремими видами кримінального аналізу, зокрема в тактичному кримінальному аналізі, але у більшості випадків кримінальний аналіз здійснюється на основі надійних даних, а не інтуїтивних висновків щодо мотивації та психологічного портрета злочинця.

Кримінальний аналіз не є кримінологічним дослідженням.

Аналітики підрозділів кримінального аналізу працюють у швидкоплинному середовищі зі складним набором даних, який змінюється щодня, створюючи інформацію, яка є прямою, терміновою для поліцейської діяльності. Незважаючи на те, що вони використовують, а іноді роблять свій внесок у офіційні кримінологічні дослідження, процеси та комплекси навичок не підлягають прямій кореляції [22, с. 7].

Досліджуючи питання щодо сутності кримінального аналізу варто також розглянути підхід групи авторів у виданні під назвою «Настільна книга поліцейського підрозділу кримінального аналізу», незважаючи на її вже історичну цінність, оскільки була видана в США у 1973 році [23].

У ній акцент зроблено на виділення так званих неформальної та формальної концепцій кримінального аналізу.

Неформальна концепція кримінального аналізу, в його найпростішому розумінні, виконується переважною більшістю детективів, слідчих чи оперативних працівників, а також їх керівництвом, тому що їх діяльність пов'язана із розслідуванням злочинів і вони постійно здійснюють якісне вивчення однієї події вчинення злочину і порівняння її з аналогічними минулими подіями. По суті, кожен детектив чи керівник підрозділу є маленьким підрозділом кримінального аналізу, оскільки він порівнює свої розслідування зі своїм минулим досвідом та досвідом інших. Однак досвід однієї особи обмежений часом його практичної діяльності, і, по суті, його узагальнення не узгоджені з узагальненнями інших.

Формальна концепція кримінального аналізу – це та, в якій відповідальність за виявлення ознак злочинів покладена на одну конкретну особу, осіб або підрозділ. Але водночас варто виділяти ступінь професійності спеціальних підрозділів кримінального аналізу. Наразі зазначають про два рівні – базовий та поглиблений. Кримінальний аналіз базового рівня характеризуються обмеженими можливостями. Тобто виконуються завдання, які покликані допомогти «вирішити» поточну проблему, а не запобігти її виникненню за допомогою прогнозів злочинності або запропонованих коригувальних програм.

Поглиблений рівень кримінального аналізу має більші можливості ніж базовий і, крім усього іншого, орієнтований на передбачення майбутніх проблем. Аналіз подій, що вже відбулися, здійснюється також і з метою виявлення майбутніх тенденцій і проблемних сегментів. Звісно, комп'ютеризація процесу кримінального аналізу є важливим компонентом сучасної організації саме поглибленого рівня. У міру того, як кримінальний аналіз стає прийнятим, вдосконаленим і поглибленим, він стане все більш оперативним інструментом, незамінним у повсякденному розгортанні особового складу.

Таким чином, характеризуючи сутність кримінального аналізу, важливим є зазначити, що

> *ще у 1973 році однією з основних функцій кримінального аналізу визначали орієнтованість на прогнозування майбутніх тенденцій.*

У виданні Ради Європи [24], присвяченому аналізу кращих практик боротьби з організованою злочинністю, також виділяється значення кримінального аналізу як інституційної складової правоохоронної діяльності та зазначається *зміст кримінального аналізу у площині найкращої практики та теорії:* кримінальний аналіз є функцією правоохоронних органів, за допомогою якої дані, що стосуються злочинності, збираються, порівнюються, аналізуються та поширюються. Простіше кажучи, – *це дослідження моделей злочинності та тенденцій у спробі розкрити злочини або запобігти їх повторенню*.

Кримінальний аналіз ґрунтується на припущенні, що злочини не є абсолютно випадковими, ізольованими та унікальними подіями, а можуть бути об'єднані в набори, що мають спільні риси та демонструють чіткі закономірності [24, с. 3]. *Кримінальний аналіз є системою, яка використовує*

регулярно зібрану інформацію про кримінальні події та причетних осіб з метою запобігання та припинення злочинів і затримання злочинців [23].

Наразі сучасний підхід до тлумачення змісту кримінального аналізу є ще більш широким. У Білій книзі від 2014 року Міжнародної асоціації аналітиків злочинності (*IACA*) визначено узагальнений підхід, за яким ***кримінальний аналіз*** *– це професія та процес, у яких використовується комплекс кількісних і якісних методів для аналізу даних, що мають цінність для правоохоронних структур та їхніх громад. Він охоплює аналіз злочинів і злочинців, жертв злочинів, порушень громадського порядку, проблем якості життя, проблем дорожнього руху та внутрішніх операцій поліції, а його результати підлягають використанню в кримінальних розслідуваннях і кримінальному переслідуванні, патрульній діяльності, стратегіях запобігання та скорочення злочинності, а також для розв'язання проблем та оцінювання ефективності діяльності поліції [22, с. 6].*

У визначенні уточнено, що:

- ✓ *весь аналіз даних, що здійснюється в правоохоронних органах (із врахуванням усіх правоохоронних функцій, зокрема: патрульної, слідчої, превентивної, сервісної та екстреного реагування тощо), підпадає під категорію «кримінальний аналіз»;*
- ✓ *наголошено, що слово «кримінальний» у словосполученні «кримінальний аналіз» не потрібно сприймати буквально, тобто аналітики досліджують усі дані, важливі для поліції;*
- ✓ *кримінальний аналіз забезпечує підтримку всіх основних функцій у правоохоронній діяльності.*

Для того, щоб краще розуміти зміст кримінального аналізу Джеррі Ретклiфф (*Jerry H. Ratcliffe*) у своїх публікаціях зазначає, що *з огляду на мету дослідження як кримінальних подій, так і більш широких тенденцій в структурі злочинності, якісний кримінальний аналіз повинен базуватися на розумінні широкого спектру технічних та теоретичних аспектів [11].*

Наприклад, досвідчений аналітик може мати розуміння та використовувати навички щодо кількісних досліджень за допомогою різноманітних програмних продуктів, зокрема, використовувати географічну інформаційну систему для просторово-часового аналізу злочинності, створювати аналітичні продукти та проводити брифінги для працівників поліції. Проте іноді загальне розуміння обмежується лише тим, що аналітики просто надають керівництву схеми та розбивки простих підрахунків кількості різних типів злочинів, що відбулися за останній тиждень. ***Ці завдання не є кримінальним аналізом, а просто представляють собою управлінську статистику****. Такого роду специфіка роботи аналітика, що не пов'язана з процесом вирішення проблем зниження рівня та запобігання злочинності, може значною мірою пом'якшувати ентузіазм деяких аналітиків.*

Аналітики можуть використовувати нелінійні підходи до аналізу, синтезуючи інформацію, отриману за рахунок використання різноманітних методів, задля більш повного та цілісного бачення проблеми злочинності. Ці методи можуть включати мапування злочинів, статистичний аналіз, польові спостереження за регіонами з високим рівнем злочинності та низьким рівнем злочинності, аналіз звітів про злочини та розвідувальних даних, спілкування з офіцерами, підозрюваними та жертвами, пошук посилань на докази, а також збір інформації про відомих правопорушників тощо [11].

Водночас ***важливими є висновки Джеррі Ретклiффа*** як авторитетного та відомого фахівця, до яких варто прислухатися –

> *хороший кримінальний аналіз є функцією управління змінами поліцейського менеджменту. Саме тому якісний кримінальний аналіз потребує інвестицій у навчання, апаратні засоби, програмне забезпечення та персонал, щоб функціонувати на більш високих рівнях далеко від базового статистичного менеджменту.*

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Про бюро економічної безпеки України: Закон України від 28 січ. 2021 р. № 1150-IX. URL: https://zakon.rada.gov.ua/laws/show/1150-20#Text
2. Про запровадження системи управління ризиками та системи кримінального аналізу у Державній прикордонній службі України: наказ Адміністрації Держприкордонслужби України від 21 лют. 2007 р. № 130.
3. Про затвердження Інструкції про організацію та ведення кримінального аналізу оперативно-розшуковими підрозділами: наказ Адміністрації Держприкордонслужби України від 15 січ. 2008 р. № 28.
4. Сергєєва Г.А. Англомовні запозичення в українській правничій термінології: дис. … канд. філол. наук: 10.02.01. Харків, 2002. 250 с.
5. Кіреєва О.С., Крутік Ю.В., Махлай О.М., Треус А.С. Основи кримінального аналізу: теорія та практика застосування в оперативних підрозділах Державної прикордонної служби України: навчальний посібник. Хмельницький: Вид-во НАДПСУ, 2022. 388 с.
6. Манжос Я.Ю. Семантичні та функціональні особливості англомовних юридичних термінів – назв злочинів проти людини: автореф. дис. … канд. філол. наук: 10.02.04 / Харк. нац. ун-т ім. В.Н. Каразіна. Харків, 2011. 20 с.

7. Олійник О. Юридичні терміни як вербальні репрезентанти правового концепту. *Наукові записки. Серія: Філологічні науки*. 2018. Вип. 165. С. 331-338.
8. Главацька Ю. Термінологічне поле vs терміносистема: принципи наповнення та структурації термінологічного поля в мові. *Науковий вісник Херсонського державного університету. Серія: Лінгвістика*. 2014. № 21. С. 15-18.
9. Ляшук А.М. Семантична структура юридичних термінів української та англійської мов: дис... канд. філол. наук: 10.02.17 / Кіровоградський держ. педагогічний ун-т ім. В. Винниченка. Кіровоград, 2007. 335 с.
10. Вікіпедія. URL: https://uk.wikipedia.org/wiki/
11. Ratcliffe, J.H. (2007). Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders. US Department of Justice. Office of Community Oriented Policing Services. Washington, DC.
12. Іващенко В.Л., Василькова Л.М. Кримінальний Кодекс України – Карний Кодекс України. *Кримінально-процесуальний Кодекс України – Карно-процесуальний Кодекс України*: Термінологічний вісник. 2013. Вип. 2(2). С. 185-187.
13. Словник іншомовних слів / За ред. акад. О. С. Мельничука. Київ, 1977. 775 с.
14. IASA. Retrieved from https://www.iasa.net/certification
15. Boba, R. (2003). *Problem Analysis in Policing*. Washington, DC: Police Foundation.
16. Scott, M.S. (2000). *Problem-Oriented Policing: Reflections on the First 20 Years*. Washington, DC: Office of Community Oriented Policing Services.
17. Eck, J.E., & Spelman, W. (1987). *Problem Solving: Problem-Oriented Policing in Newport News*. Washington DC: Police Executive Research Forum.
18. Emig, M., Heck, R., & Kravitz, M. (1980). *Crime analysis: A selected bibliography*. Washington, DC: U.S. National Criminal Justice Reference Service.
19. Steven, Gottlieb, Sheldon, Arenberg & Raj, Singh (1994). *Crime analysis from first report to final arrest*. Alpha, Montclair, Calif. California.
20. Karim, Vellani & Joel, Nahoun (2001). *Applied crime analysis*. Butterworth-Heinemann. United States of America.
21. Boba, R. (2005). *Crime Analysis and Crime Mapping*. Thousand Oaks, CA: Sage.
22. K. Gallagher, J. Wartell, S. Gwinn, G. Jones, & G. Stewart (eds.) (2017). *Exploring crime analysis: Readings on essential skills* (3rd ed.). International Association of Crime Analysts. Overland Park, KS.
23. George A., Buck (proj. direct.), Robert Austin John, Hodges, Gary Cooper Kai, Martensen & Don Gagnon Michael, O'neal (1973). *Police crime analysis unit handbook.* U.S. Department of Justice National Institute of Justice U.S. Government Printing Office Washington.
24. Council of Europe. Crime analysis. Organized crime - Best Practice (2002). №4 PC-S-CO. 2E Strasbourg, 22 July 2002.

DOI: https://doi.org/10.36486/978-966-2310-66-5-12

Розширювати свої знання можна тільки тоді, коли дивишся прямо в очі власному незнанню.

Костянтин Ушинський

РОЗДІЛ 12
Типології кримінального аналізу

Олександр Користін
Дмитро Афонін
Владислав Бурангулов
Ігор Федчак

З'ясування змісту кримінального аналізу доречно продовжити, розклавши його на певні види, які відрізняються, зокрема за метою, характером, обсягом та джерелом даних, застосованими методами аналізу, результатами, регулярністю і частотою аналізу, а також цільовою аудиторією тощо.

Наразі, серед фахівців та дослідників використовується досить різноплановий підхід щодо зазначеної типології за видами кримінального аналізу.

> *Жодна типологія ніколи не претендує на вичерпний набір визначень. Нерідко має місце частковий збіг у визначеннях змісту різних видів кримінального аналізу, залежно від обставин, а також появи нових ідей і технік [1, IACA].*

Ще до початку 1980-х рр. багато різноманітних програм, спрямованих на зниження рівня злочинності, були об'єднані в Інтегровану програму затримання злочинців (*ICAP*). І саме у цій інтегрованій програмі кримінальний аналіз займав окреме місце. Водночас вперше саме у цій програмі було визначено чотири типи аналізу:

- кримінальний аналіз *(crime analysis),*
- розвідувальний аналіз *(intelligence analysis),*
- аналіз даних розслідувань *(investigative analysis) та*
- аналіз операцій *(operations analysis).*

В Україні вже тривалий час має місце дискусія щодо визначення видів (типів) кримінального аналізу, а тому, зазначаючи про типи кримінального аналізу, що були визначені Інтегрованою програмою у 1980-х роках в Сполучених Штатах, ми спеціально їх подали і мовою оригіналу.

Водночас, завдання щодо формування загального розуміння видів кримінального аналізу допомагає зосередити фокус на різних видах діяльності аналітиків, у підготовці аналітиків та їх навчанні, підтримці професійної діяльності на основі визначення посадових інструкцій, завдань та обов'язків.

Зокрема, мислення в категоріях видів кримінального аналізу допомагає професії аналітика кількома способами:

- ✓ *гарантування повного спектру аналітичних послуг;*
- ✓ *визначення сфер, які потребують аналітичного розвитку та реагування аналітиків;*
- ✓ *визначення сфер для розвитку професійних знань та навичок аналітиків, їх навчання та формування професійної літератури;*
- ✓ *планування щоденних, тижневих, місячних та річних завдань;*
- ✓ *класифікацією аналітичних продуктів та планування графіків їх розповсюдження;*
- ✓ *визначення відповідних технік та інструментів щодо конкретних цілей аналізу.*

Перш за все, звертає на себе увагу типологія, визначена IACA [2], яка розрізняє чотири основних види кримінального аналізу:

тактичний кримінальний аналіз *(tactical crime analysis);*
стратегічний кримінальний аналіз *(strategic crime analysis);*
кримінальний розвідувальний аналіз *(crime intelligence analysis);*
управлінський (адміністративний) аналіз злочинності *(administrative crime analysis).*

В інших джерелах, посилаючись на IACA [3; 4], виділяється лише три види КА, хоча в різній послідовності:

тактичний кримінальний аналіз *(tactical crime analysis);*

стратегічний кримінальний аналіз *(strategic crime analysis);*
управлінський (адміністративний) аналіз злочинності *(administrative crime analysis).*

У свою чергу, відомий фахівець у цій сфері, професорка Редфордського університету Рейчел Боба Сантос (*Rachel Boba Santos*) у своїй книзі «*Crime Analysis with Crime Mapping*» 2006 року видання [5] та інші джерела [6; 7; 8] виділяють п'ять видів кримінального аналізу:

Intelligence Analysis
Criminal Investigative Analysis
Tactical Crime Analysis
Strategic Crime Analysis
Administrative Crime Analysis

А вже у 2022 році, у перевиданій книзі «*Crime Analysis with Crime Mapping*» Р. Боба [9] виділяє лише чотири види кримінального аналізу, які повністю корелюються з підходом IACA, видаливши з переліку «*Criminal Investigative Analysis*».

Особливим є підхід до визначення та виділення видів кримінального аналізу в INTERPOL [10; 11], де застосовується специфічний термін «*Criminal intelligence analysis*».

> *Термін «Criminal intelligence analysis» наповнює кримінальний аналіз додатковим змістом «Intelligence», що може інтерпретуватися як кримінальний розвідувальний аналіз та вказує на концептуальний зв'язок з Intelligence-led Policing.*

Розкриваючи історичну генезу розвитку кримінального аналізу, було зазначено саме на цій особливості сучасного наповнення змісту діяльності підрозділів кримінального аналізу. Водночас INTERPOL виділяє оперативний (або тактичний) та стратегічний аналіз.

Різноманітність підходів щодо типології кримінального аналізу є плинною та змінюється, розвиваючись у контексті нового змісту кримінального аналізу та особливо домінуючої моделі правоохоронної діяльності. Це стосується й сучасної моделі правоохоронної діяльності, керованої аналітичною розвідкою (Intelligence-led Policing), яка передбачає інкорпорування аналітичної розвідувальної функції в загальну місію правоохоронної системи.

> *Комплексне завдання – прогнозування ризиків та вплив на дії – передбачає комбінування аналізу та процесу прийняття рішень, що створює додаткові виклики для спеціалістів розвідувальних аналітичних служб [12, с. 25].*

Із врахуванням сучасної моделі у посібнику ОБСЄ «Guidebook Intelligence-Led Policing» [13] зазначається: *«Як і у випадку з різними типами аналітики, існують різноманітні підходи щодо класифікації аналізу. Оперативний аналіз в одній установі називають тактичним аналізом в іншій, а аналіз мережі в одному поліцейському відділі називають аналізом зв'язків або схемою взаємозв'язків у сусідній країні. Найпоширенішою класифікацією аналізу є стратегічний аналіз, оперативний аналіз і тактичний аналіз».*

Такий підхід є ключовим і у публікаціях найбільш цитованого вченого з питань змісту, розуміння та імплементації Intelligence-led Policing – доктора Джеррі Ретклiффа (*Dr. Jerry H. Ratcliffe*), який виділяє три рівні аналітичної розвідки (Intelligence): *стратегічний, оперативний, тактичний* і саме у такій послідовності [14].

Д-р Джеррі Ретклiфф зазначає, що традиційний підхід полягає у визначенні двох або трьох площин аналітичної діяльності [15]:

> ***тактична** – підтримка оперативних підрозділів, розслідувань та інших підрозділів у вжитті конкретних заходів для досягнення цілей правозастосування,*
>
> ***оперативна** – підтримка керівників підрозділів і регіональних органів у плануванні заходів зі зниження рівня злочинності та розподілі ресурсів,*
>
> ***стратегічна** – спрямована на забезпечення розуміння, а також внеску у широкі стратегії, політики та ресурси.*

Більшість організацій використовують певні варіації цих описів, але іноді досить безсистемно: деякі з них не мають оперативного рівня тоді як інші описують свій тактичний рівень як оперативний тощо [15].

Таким чином, подальший аналіз необхідно зосередити на змістовній характеристиці кожного із зазначених видів, з'ясувавши особливості, відмінності та сформувавши бачення щодо оптимальної на сьогодні типології, що найбільше відповідає потребам правоохоронних органів України. Водночас, важливо ще раз зазначити, що такий підхід до визначення видів кримінального аналізу повністю корелюється з моделлю Intelligence-led Policing, а також є традиційним у професійному сприйнятті працівниками органів правопорядку, державної безпеки та військових формувань в Україні.

СТРАТЕГІЧНИЙ КРИМІНАЛЬНИЙ АНАЛІЗ

У різних джерелах містяться різні підходи до визначення та характеристики стратегічного кримінального аналізу. Перш за все, звертає на себе увагу обґрунтування змісту стратегічного кримінального аналізу, викладене у виданні IACA [2]:

> *Стратегічний кримінальний аналіз фокусується на довгострокових тенденціях, проблемах та «гарячих точках» злочинності й порушень громадського порядку.*

Стратегічний кримінальний аналіз є періодичним, а не щоденним обов'язком. Аналіз тенденцій, проблем та гарячих точок починається з наявних даних поліції. Однак загалом дані поліції є недостатніми для пояснення першопричин та основних факторів можливостей, пов'язаних із цими довгостроковими явищами. Для цього аналітики звертаються до збору якісних дані, які виходять за рамки поліцейського звіту. Ці якісні методи, включаючи інтерв'ю, опитування, фокус-групи, експертні оцінки та зовнішні дослідження [2, с. 12].

Професорка Редфордського університету Рейчел Боба Сантос (*Rachel Boba Santos*) у виданні 2006 року [5, с. 15] зазначає, стратегічний кримінальний аналіз – *це вивчення проблем злочинності та інших питань, пов'язаних із завданнями поліції, для визначення довгострокових моделей діяльності, а також для оцінки реагування поліції та організаційних процедур.*

Двома основними цілями стратегічного кримінального аналізу є
допомога у виявленні та дослідженні довгострокових проблем злочинності та
оцінка реагування поліції на проблеми та організаційні процедури поліцейських установ.

Вивчення проблем може включати аналіз рівня злочинності, повторної віктимізації, гарячих точок і характеристик середовища, які впливають на можливості та випадки злочинів. Результати стратегічних досліджень аналітиків та оцінка реакції поліції на проблеми злочинності допомагають поліцейським службам оцінювати їхню ефективність.

А у виданні 2022 року Рейчел Боба [9, с. 15] вказує на те, що *метою стратегічного кримінального аналізу є виявлення довгострокових проблем і розуміння, чому вони виникають, для спрямування ресурсів поліції на розробку довгострокових рішень*.

Подібно до тактичного кримінального аналізу, дані, що використовуються для стратегічного кримінального аналізу, надходять з поліцейських баз даних, однак стратегічний аналіз злочинності часто включає збір даних з різних інших джерел, таких як дані перепису населення, дані географічного районування та дані про міста, а також може включати первинні дані, зібрані як кількісними, так і якісними методами.

Крім того, стратегічний аналіз злочинності розглядає ті ж самі дані про злочинність, але в агрегованому вигляді та за більш тривалі періоди часу.

***Наприклад**, якщо тактичний кримінальний аналіз виявив, що чотири з п'яти автомобілів були відкриті в результаті крадіжок з транспортних засобів, що сталися в районі минулого тижня, то стратегічний кримінальний аналіз виявить, що 85% з 1000 автомобілів були відкриті в результаті крадіжок з транспортних засобів в цілому по місту минулого року.*

Інші джерела також вказують на особливості, що характерні для стратегічного кримінального аналізу.

Стратегічний кримінальний аналіз передбачає довгострокове вивчення інформації про злочини та її класифікацію на демографічні та просторові групи. Це допомагає у створенні кількісних моделей і дослідженні інформації. Він агрегує дані за певними періодами, як-от дані за місяць, квартал або рік. Він також надає конкретну інформацію про зібрані дані, як-от характер правопорушень, стать жертв, категорію доходу, дату, час тощо, – оскільки це допомагає створити чітку картину щодо перебігу злочинів. Основними цілями цього типу аналізу є виявлення довгострокових проблем і розробка процедури їх вирішення. Він включає оцінку різних програм, аналіз проблем та інші процедури. Можна зробити висновок, що в стратегічному аналізі використовуються статистичні механізми та методи дослідження, які потенційно можуть дати необхідні результати [5].

Важливим є підхід до обґрунтування стратегічного аналізу в INTERPOL [10; 11]: *призначений для інформування осіб, які приймають рішення на вищому рівні, і переважно реалізується в довгостроковій перспективі.*

Стратегічний аналіз включає визначення:

> *способів кримінальної діяльності;*
> *тенденцій та моделей злочинності;*
> *поширення загроз;*

> *зовнішніх факторів, таких як технологія, демографія чи економіка, що можуть потенційно вплинути на злочинну діяльність.*

Ключове завдання полягає в забезпеченні раннього попередження поширення загрози та підтримки вищого керівництва щодо визначення пріоритетів розвитку органу (підрозділу), спрямованих на вирішення нових проблем злочинності. Це може включати виділення цільових ресурсів щодо різних типів злочинів або посилення навчання певних методів протидії злочинності.

> *Стратегічний кримінальний аналіз переважно орієнтований не на затримання злочинців, а на запобігання злочинності, підвищення інституційної спроможності правоохоронних органів та зниження ризиків поширення кримінальних загроз, зокрема організованої злочинності, корупції, наркоторгівлі тощо.*

Результатом стратегічного кримінального аналізу, перш за все, є відповідна стратегія у формі нормативного акта, яка має довгостроковий регулятивний вплив в системі прийняття управлінських рішень керівництвом правоохоронного органу.

> *Стратегічний кримінальний аналіз має потенціал стати найбільш значущим аспектом аналітичної розвідки через здатність стратегічних продуктів впливати на загальну безпекову стратегію та рішення щодо використання ресурсів [16].*

Стратегічний рівень завжди страждав з точки зору досягнення легітимності, оскільки відмінність між тактичним і стратегічним *«не є лише питанням визначення або семантики, а має реальні організаційні наслідки й пронизує аналітичний процес» [17].*

Крім того, аналітик стратегічного кримінального аналізу зацікавлений у виявленні системних прогалин та вразливостей у суспільстві та того, як організовані злочинні групи використовують ці можливості.

Загалом, стратегії спрямовують свій вплив не на затримання правопорушників, а на
- *зниження привабливості об'єктів злочину та ризиків поширення кримінальних загроз,*
- *усунення причин та умов вчинення злочинів, а також на*
- *підвищення ефективності правоохоронної діяльності на основі розвитку інституційної спроможності та використання зовнішніх сприятливих факторів.*

СТРАТЕГІЧНИЙ РІВЕНЬ – забезпечує прийняття рішень, розробку політики, планування та визначення пріоритетів; розподіл ресурсів поліції; та із врахуванням видів злочинності, визначає відповідний підхід діяльності поліції; спрямовується на забезпечення уявлення щодо загроз уразливості, ризиків та можливостей щодо діяльності (оцінка загроз та ризиків) у сфері безпеки, розуміння тенденцій та системи причинно-наслідкових зв'язків, а також є внеском у розроблення широких стратегій щодо безпекової політики та використання ресурсів.

Стратегічний рівень має справжні організаційні наслідки, є базисом і пронизує весь аналітичний процес.

> *Стратегічний рівень не є терміном, пов'язаним з виняткова загальнодержавним безпековим аспектом, він також застосовується до процесу планування та розподілу ресурсів на кожному рівні (регіону) у межах безпекової політики.*

Аналітики стратегічного кримінального аналізу у своїй діяльності використовують різноманітні процеси, моделі та методи. Зокрема:

Аналіз проблемних районів (тобто «гарячих точок») – це визначення районів у межах юрисдикції з непропорційно високим рівнем злочинності порівняно з іншими районами як у часовому, так і в просторовому вимірі.

Аналіз проблем щодо правопорушників і жертв – це використання даних для виявлення та визначення пріоритетів (тобто ранжування) окремих правопорушників за кількістю, типом і тяжкістю вчинених ними злочинів, а також окремих жертв за кількістю, типом і тяжкістю їх віктимізації.

Хоча ці методи є методами аналізу оперативної інформації про злочинність, вони також застосовуються в рамках стратегічного аналізу та вирішення довгострокових проблем.

> ***Аналіз проблем*** *– це «підхід/метод/процес, що здійснюється в рамках поліцейського відомства, в якому офіційна теорія кримінального правосуддя, методи дослідження, а також комплексні процедури збору та аналізу даних використовуються в систематичний спосіб для проведення поглибленого вивчення, розробки обґрунтованих заходів реагування та оцінки проблем злочинності та порушення громадського порядку» [9].*

Він включає виявлення та визначення пріоритетності довгострокових проблем, які потребують вирішення поліцією; розуміння того, як, коли, де, хто і чому виникає проблема; управління заходами реагування на проблему; та оцінку ефективності заходів реагування.

Аналіз тенденцій включає агрегування даних про злочинність та інших поліцейських даних, як правило, за періодом часу (наприклад, місяць) та географічною територією (наприклад, район, область) з метою виявлення зростання або зниження рівня злочинності. Статистичні дані є відносно простими і зрозумілими, але методи спрямовані на об'єднання даних у категорії та використання різних статистичних даних для вивчення тенденцій (наприклад, рівень насильницьких злочинів за роками, середня кількість пограбувань на місяць; відсоткова зміна кількості квартирних крадіжок у районі). Аналітики готують статистичні дані, які включають регулярні аналітичні звіти, що підтримують зустрічі та процеси підзвітності відомства у сфері зниження рівня злочинності. Продукти для підзвітності, як правило, дещо відрізняються від тих, що використовуються для виявлення, розуміння та оцінки окремих проблем.

У стратегічному кримінальному аналізі *мапування злочинності* використовується в довгострокових програмах, таких як:

(1) аналіз взаємозв'язку між злочинною діяльністю та індикаторами порушення громадського порядку (виклики поліції до місць порушення громадського порядку);

(2) вивчення активності в певних місцях або навколо них, таких як школи, бари або центри лікування наркозалежності;

(3) обчислення інформації про рівень злочинності в межах невеликих географічних районів (наприклад, кількість квартирних крадіжок до кількості домогосподарств);

(4) визначення конкретних районів з непропорційно високим рівнем злочинності (тобто, проблемних районів).

Процес SARA є найбільш відомим у практичному використанні в стратегічному кримінальному аналізі. SARA передбачає (*scanning, analysis, response, assessment*):

– сканування *(scanning): виявлення повторюваних проблем та наслідків впливу на безпеку громад;*

– аналіз *(analysis): збір та аналіз усіх відповідних даних про проблему з метою зясування шляхів впливу на причини виникнення проблеми;*

– реагування *(response): пошук відповідей, які могли б працювати в інших місцях, виявлення низки місцевих варіантів, а потім вибір і здійснення конкретних заходів, які дозволять вирішити проблему;*

– оцінка *(assessment): перевірка даних, зібраних до і після етапу реагування, з метою визначення, чи зменшило реагування проблему, а якщо ні, то визначити нові стратегії, які можуть спрацювати. нових стратегій, які можуть спрацювати.*

Із врахуванням сучасної моделі у посібнику ОБСЄ «Guidebook Intelligence-Led Policing» зазначається, що потреба в аналітиці обумовлена процесом стратегічної оцінки [13].

> *Оцінка дає керівникам правоохоронних органів огляд проблем поліції, з якими стикається або може зіткнутися установа. Підготовлений аналітичним підрозділом цей широкий документ, відображає національні, регіональні та місцеві стратегічні пріоритети. Підготовка документа є першим етапом у процесі стратегічного планування.*

Усі існуючі та нові загрози, виявлені під час процесу сканування стратегічної оцінки, мають бути розглянуті в документі. Не можна упускати жодної значної деталі. Далі документ розглядається на стратегічному форумі, у форматі якого виявлені загрози розглядаються в контексті наявних ресурсів. Пріоритети зіставляються із ресурсами. Кількість загроз, включених до будь-якої стратегії контролю, визначається ресурсами, доступними для їх вирішення; ті, яким стратегічний форум надає найвищий пріоритет, включаються до стратегії контролю. Це встановлює оперативний порядок денний, який, у свою чергу, контролюється керівниками середньої ланки, які несуть особисту відповідальність за кожний із виявлених пріоритетів і зобов'язуються сформулювати плани управління цими загрозами.

Стратегія контролю містить поєднання національних, регіональних і місцевих пріоритетів, щоб вона могла включати явища, які інакше здавалися б не пов'язаними між собою, такі як міжнародний тероризм, вуличне пограбування та водіння в нетверезому стані. Стратегія має залишатися незмінною до підготовки наступної стратегічної оцінки або до виявлення більш суттєвих загроз та доведення до відома керівництва. Оперативні/тактичні оцінки, представлені на регулярних оперативних/тактичних нарадах, забезпечують залишення цих пріоритетів у центрі уваги установи.

Оперативні/тактичні наради переглядають оперативні плани, розроблені менеджерами середньої ланки та створюють форум для обговорення нових загроз. Це є гарантією того, що менеджери зосереджуються на визначених керівниками загрозах.

Інші загрози, визначені в стратегічній оцінці, не слід ігнорувати, навіть якщо немає достатніх ресурсів; вони додаються до стратегії контролю і залишаються у полі зору аналітиків. Усі працівники правоохоронних органів зобов'язані визначати пріоритети своєї роботи відповідно до стратегії контролю.

ОПЕРАТИВНИЙ КРИМІНАЛЬНИЙ АНАЛІЗ

Багато поліцейських органів, підрозділів та й деякі аналітики не визнають оперативного рівня кримінального аналізу, однак це одна із найбільш швидкозростаючих сфер управління інформацією в поліції [15]. Знаходячись між сфокусованою на правопорушниках тактичною ареною та стратегічним рівнем щодо формування стратегії, політики та довгострокових планів, оперативний кримінальний аналіз, який може сприяти зниженню масштабів загроз у регіонах та плануванню відповідних ресурсів, безсумнівно, є ключовим компонентом [18].

Д-р Джеррі Ретклiфф зазначає, що

> *на оперативному рівні кримінального аналізу аналітики переймаються структурою злочинності, кластеризацією діяльності, з метою визначення проблемних питань для діяльності правоохоронного підрозділу [18].*

На оперативному рівні кримінальний аналіз вирішує питання прийняття рішень, що пов'язані з управлінням програмами, галузевими правоохоронними кампаніями, керівниками регіонального рівня і, як правило, цей процес обмежується роком. На цьому рівні аналітичний процес спрямовується на визначення та вивчення тенденцій та проблем, пов'язаних з однією чи кількома правоохоронними програмами (кампаніями). Програми оперативного рівня прийняття рішень, можуть бути в значній мірі згруповані за трьома основними потоками роботи [19]: *аналіз патернів, оцінка загроз, спеціалізовані програми збору даних.*

Програми аналізу патернів можуть бути визначені за конкретною темою або наявною проблемою. Вони також можуть бути визначені за геопросторовим принципом (місцезнаходженням, регіональністю), або, можливо, цільовими групами, які представляють певний інтерес. Там, де аналітики об'єднуються в такі програми, важливою характеристикою є попередня визначеність її шляхом стратегічного кримінального аналізу.

Важливим акцентом у реалізації програми аналізу патернів є участь у ній аналітиків, які обізнані з аналітичними методиками на рівні вищому від базового, бо їхня увага зосереджується на активному використанні додаткових специфічних джерелах інформації, вони розглядають більш широкі тенденції ніж на тактичному рівні, не обмежуються аналізом окремих об'єктів, а намагаються будувати більш складні моделі. Аналітики на оперативному рівні повинні на певному етапі бути занурені в зважування рівня загрози з боку різних груп або окремих осіб, а також їх фактичного або потенційного впливу.

Цільовим об'єктом оперативного кримінального аналізу розглядаються групи високого ризику як для конкретної діяльності, так і, загалом, типи чи форми активності, що характеризуються наявністю чи потенційною загрозою. Зазвичай показники для них встановлюються за допомогою спільної моделі оцінки ризику.

Як пояснює Ван дер Бекен [20], оперативний кримінальний аналіз слід проводити на системній груповій основі, а не як аналіз кожного окремо аналітика. Система повинна з'ясувати як різноманітні складові елементи, пов'язані з моделями поведінки та діями, які формуються в умовах навколишнього середовища. Він стверджує, що увага повинна зосереджуватися на аналізі взаємозв'язків, взаємозалежності, а не на сутностях.

> *Тенденції, які впливають на навколишнє середовище або організовану групу, і способи взаємодії цих елементів є головним завданням, оскільки прогнозні моделі залежать від їх здатності продемонструвати зв'язки між ідентифікованими незалежними змінними та залежною змінною.*

Найважливішим досягненням в програмах аналізу оперативного рівня є підтримка можливостей збору даних зі здатністю штучного інтелекту. Програми штучного інтелекту є витонченими, їх можна використовувати на основі достатності досягнення статистичної значущості. Перевага полягає в тому, що ці програми постійно розвивають аналітичні можливості та поступово можуть виходити на рівень аномальних профілів.

Мистецтво аналізу патернів потребує більше креативності, а не програмування шаблонів: за часом, за подіями або їх поєднаннями.

Програми оцінки загроз також базується на груповому аналізі й відправним моментом є поняття «загроза», яка часто переплітається з поняттям «шкода». Аналітичний процес розпочинається з розгляду рівня генерування шкоди та оцінки груп людей, які створюють шкоду. Певним чином поняття «загроза» можливо замінити терміном «профіль».

Програма оцінки загрози спрямована на створення надійної, динамічної системи для оцінки потенційних загроз та, порівнюючи їх, визначення пріоритетності цих загроз. Це дозволяє приймати обґрунтовані рішення щодо оперативних пріоритетів розподілу ресурсів та зусиль на всіх рівнях для контролю або усунення цих загроз. На оперативному рівні керівництво правоохоронного органу здатне визначити найбільш доцільне використання ресурсів і які пріоритети є найбільш актуальними. Діяльність, пов'язана з наркотиками та організованою злочинністю, може оцінюватися разом із питаннями контролю за дотриманням правил дорожнього руху та громадського порядку в середовищі, де розподіляються ресурси на основі більш широких потреб громади та повного знання можливостей відділу.

Із врахуванням сучасної моделі у посібнику ОБСЄ «Guidebook Intelligence-led Policing» [13] зазначається щодо мети кримінального аналізу на оперативному рівні:

> *допомога управлінню для досягнення оперативних цілей; підтримка регіональних керівників, територіальних підрозділів у плануванні діяльності щодо зменшення масштабів злочинності та розгортання ресурсів для досягнення оперативних цілей.*

ТАКТИЧНИЙ КРИМІНАЛЬНИЙ АНАЛІЗ

Тактичний кримінальний аналіз – передбачає аналіз даних, що спрямований на визначення короткострокових пріоритетів щодо патрулювання та досудового розслідування й розподілу ресурсів. Це процес, що здійснюється систематично та зорієнтований на конкретні заходи, які патрульні та слідчі підрозділи виконують щоденно для розв'язання поточних проблем, пов'язаних зі злочинністю та громадською безпекою. Особлива увага зосереджується на встановленні типової поведінки правопорушників, узагальненні способів та моделей (патернів) вчинення кримінальних правопорушень.

Цей вид аналізу потребує постійної актуалізації інформації за рахунок наповнення новими даними і на здійснення заходів з тактичного аналізу може припадати більшість робочого часу аналітиків.

У межах тактичного кримінального аналізу здійснюється узагальнення отриманих даних та поширюється відповідна інформація серед визначених працівників правоохоронного органу для подальшого прийняття оперативного рішення щодо вчинених кримінальних правопорушень, отриманих актуальних даних від інших правоохоронних органів, а також щодо рецидивних інцидентів (серії злочинів або викликів, пов'язаних з одними й тими ж місцями та причетними особами). Готуються звіти та мапи для підтримки тактичних операцій.

> *Але більшість тактичних прийомів і зусиль в межах тактичного кримінального аналізу зосереджуються на встановленні моделей (патернів) кримінальної діяльності [2, IACA].*

IACA орієнтує на модель, в основі якої унікальність двох або більше кримінальних правопорушень ідентифікується через відповідність кожній з визначених умов [2]:

- *спільною для них є хоча б одна ознака щодо виду злочину; поведінки правопорушників або жертв; характеристики правопорушників, жертв або об'єктів; привласненого майна або місця, де їх було вчинено;*
- *невідомо про зв'язки між жертвою (жертвами) і правопорушником (правопорушниками);*
- *спільні риси чітко вирізняють сукупність кримінальних правопорушень серед інших, вчинених у межах одного й того самого часового проміжку;*
- *кримінальна активність переважно має обмежену тривалість – від кількох тижнів до кількох місяців;*
- *сукупність пов'язаних кримінальних правопорушень розглядається як один об'єкт кримінального аналізу та зосередження зусиль і тактичних дій поліції.*

Найчастіше аналітики використовують метод щоденного аналізу даних й інформації про кримінальні правопорушення та їх подальше порівняння з минулими інцидентами. Порівнюючи, аналітик встановлює достатність спільних рис між минулим і поточним інцидентом, а також ймовірність певної закономірності вчинення кримінальних правопорушень. З цією метою використовуються бази даних й відповідні пошукові сервіси, мапування кримінальних правопорушень та статистичні методи (наприклад, аналіз порогових значень), які допоможуть ідентифікувати патерни.

Професорка Рейчел Боба Сантос тактичний кримінальний аналіз визначає таким чином [5]:

> *тактичний кримінальний аналіз – це вивчення нещодавніх кримінальних подій і потенційної злочинної діяльності шляхом вивчення таких характеристик, як те, як, коли і де відбулася дія, щоб допомогти у розробці моделей (патернів), слідчих дій та ідентифікації підозрюваних, а також розкритті справи.*

Тактичний кримінальний аналіз зосереджується на недавніх злочинах і на конкретній інформації про методи злочинів, а також про залучених осіб і транспортні засоби. Проаналізовані дані отримані з офіційних звітів поліції, які включають інформацію про характеристики злочинів, такі як спосіб проникнення, місце входу, дії підозрюваного, тип жертви та тип використаної зброї, а також дата, час, місце, і тип розташування. Типи злочинів, які зазвичай розглядаються в тактичному кримінальному аналізі, це ті, у яких злочинець не знає жертви, і ті, щодо яких є адекватна інформація про злочин (спосіб злочину) для аналізу.

Р.Боба також вказує на три цілі які має тактичний кримінальний аналіз:
- *зв'язати злочини та таким чином виявити моделі (патерни);*
- *виявити потенційних підозрюваних у злочинах або моделі (патерни) злочинів;*
- *зв'язати розкриті злочини з відкритими справами та таким чином допомогти розкрити чи закрити справи.*

Професорка пояснює, що поліцейські та детективи витрачають більшу частину часу на розслідування окремих справ, вони часто не встигають зробити крок назад, щоб виявляти закономірності, моделі (патерни) злочинів. Тактичний кримінальний аналіз – це процес повернення цього кроку назад:

> *«Досліджуючи багато злочинів разом, аналітики тактичного кримінального аналізу можуть ідентифікувати закономірності, а також допомогти зв'язати моделі з потенційними правопорушниками» [5].*

У виданні 2022 року «Crime Analysis with Crime Mapping» [9] професорка Рейчел Боба Сантос метою тактичного кримінального аналізу визначає виявлення короткострокових моделей діяльності. Різні типи злочинів пов'язані між собою за типом діяльності, місцем, правопорушником, жертвою, майном і способом вчинення злочину.

Методи і процеси, які використовуються для тактичного аналізу злочинів, включають:
- *аналіз повторюваних інцидентів,*
- *аналіз моделей (патернів) злочинності,*
- *аналіз кримінальних розслідувань,*
- *географічне профілювання.*

Аналіз повторюваних інцидентів – це використання даних про виклики поліції для виявлення місць, де протягом короткого періоду часу відбувалися подібні виклики, щоб спрямувати поліцейські ресурси на місця «повторних викликів».

Аналіз моделей злочинності – це використання даних звітів про злочини для виявлення груп злочинів, які певним чином пов'язані між собою, щоб спрямувати ресурси поліції на запобігання майбутнім злочинам та/або затримання злочинця(ів). Зв'язок відомих злочинців з минулими злочинами пов'язаний з аналізом моделей і полягає у використанні даних про осіб, які були заарештовані та/або засуджені за певний злочин, для того, щоб пов'язати їх з окремими злочинами або моделями злочинів. Метою аналізу структури злочинів є спрямування ресурсів поліції, затримання особи та/або розкриття однієї чи кількох справ шляхом арешту.

Аналіз моделі, як правило, зосереджується на тих факторах (хто, що, коли, де або як), які є спільними для значної кількості інцидентів. Виявлення цих спільностей часто є ключем до вирішення шаблону.

> ***Наприклад**, у схемі вуличного пограбування, в якій кожен інцидент має однаковий опис злочинця (серія), аналітик може зосередитися на правопорушнику, шукаючи базу даних відомих правопорушників, які відповідають цьому опису. У схемі крадіжки зі зламом, в якій крадуть східні килими, рішення може полягати в пошуку торгових точок для вкрадених килимів. Схема вихоплення гаманця, локалізована в одній частині парку, може бути недопущена за допомогою певного перепроектування. Якщо інциденти в серії часових інтервалів або географічних спільних рис, аналітик може спробувати спрогнозувати, де і коли порушник завдасть наступного удару [2].*

Аналіз кримінальних розслідувань передбачає процес побудови «профілів» злочинців, які вчинили тяжкі злочини, зокрема зґвалтування або вбивства. У 1970-х і 1980-х роках цей вид аналізу називався кримінальним профілюванням (*criminal profiling*), але зловживання ним у телевізійних шоу і фільмах змусило ФБР змінити термін [9]. Використовуючи елементи серії злочинів, аналітик визначає характеристики невідомого злочинця, такі як наркотична залежність, соціальні звички та місце роботи, з метою ідентифікації та визначення пріоритетності підозрюваних, щоб підтримати та допомогти слідчим у розслідуванні.

Як зазначає IACA [1, с. 7], *«У тій мірі, в якій кримінальне «профілювання» або аналіз кримінальних розслідувань відбувається в місцевих органах поліції, ми (члени IACA) розглядаємо його як невід'ємну частину процесу тактичного аналізу, оскільки він майже завжди зосереджується на серії злочинів».*

> ***Географічне профілювання*** *є частиною аналізу кримінального розслідування, а отже, також підпадає під сферу тактичного кримінального аналізу. Аналітик використовує географічні місця вчинення злочинів злочинцем (наприклад, місця скидання тіл або місця зустрічей), щоб визначити та позначити пріоритетні райони, де, ймовірно, проживає злочинець (Rossmo, 2000, 2012). Знову ж таки, мета полягає в тому, щоб ідентифікувати та затримати невідомого серійного злочинця.*

У тактичному кримінальному аналізі мапування злочинів використовується для виявлення закономірностей, пов'язаних з близькістю інцидентів. Мапування злочинності особливо корисне для виявлення моделей майнових злочинів та вуличних пограбувань. Наприклад, просторовий аналіз випадків викрадення автомобілів може виявити кластери активності в певних місцях, які можуть вказувати на схему злочину.

> *У географічному профілюванні мапування злочинності та просторовий аналіз місць вчинення злочинів є центральними.*

ВИКОРИСТАНІ ДЖЕРЕЛА

1. International Association of Crime Analysts (IACA). *Definition and Types of Crime Analysis*. Standards, Methods, & Technology (SMT) Committee White Paper 2014-02. October 2014.
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, KS.
3. *Types of Crime Analysis Essay*. Retrieved from https://ivypanda.com/essays/types-of-crime-analysis/
4. *Types of Criminal Analysis*. Retrieved from https://beavertonpolice.org/DocumentCenter/View/60/ Types-of-Crime-Analysis
5. Rachel Boba, Santos (2006). *Crime Analysis with Crime Mapping*. SAGE Publications, Inc.
6. *Crime Analysis Defined.* Retrieved from https://www.sagepub.com/sites/default/files/upm-binaries/6243_Chapter_2__Boba_Final_PDF_2.pdf
7. *Fundamentals of crime analysis*. Retrieved from https://blog.ipleaders.in/fundamentals-crime-analysis/
8. Rachel Boba, Santos (2001). *Introductory Guide to Crime Analysis and Mapping*. Office of Community Oriented Policing Services (COPS). Conference Material. Washington, DC.
9. Rachel Boba, Santos (2022). *Crime Analysis with Crime Mapping*. SAGE Publications, Inc.
10. *Interpol*. Retrieved from https://www.scribd.com/document/406786777/dbhhgh-fbhbhf-fhnj
11. *Interpol. Criminal intelligence analysis*. Retrieved from https://www.interpol.int/How-we-work/ Criminal-intelligence-analysis2
12. Користін О.Є., Пефтієв Д.О., Пеньков С.В., Некрасов В.А. *Довідник керівника поліції - поліцейська діяльність, керована розвідувальною аналітикою* / ILP. Київ: «Видавництво Людмила», 2019. 120 с.
13. *OSCE Guidebook Intelligence-Led Policing* (2017). TNTD/SPMU Publication. Series Vol. 13. Vienna.
14. Jerry H., Ratcliffe (2007). *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders*. Police Foundation. Washington, DC.
15. Jerry H., Ratcliffe (2016). Intelligence-Led Policing. Second edition. New York: Routledge.
16. John, Tim & Mike, Maguire (2003). *Rolling out the National Intelligence Model: key challenges.* In Crime Reduction and Problem-oriented Policing, edited by Karen Bullock and Nick Tilley, 38-68. Cullompton, Devon: Willan Publishing.
17. Gill, Peter (2000). *Rounding up the usual suspects? Developments in contemporary law enforcement intelligence*. Aldershot: Ashgate.
18. Quarmby, Neil. 2009. Futures work in strategic criminal intelligence. *In Strategic Thinking in Criminal Intelligence* (2nd edition), edited by Jerry H. Ratcliffe. Sydney: Federation Press.
19. Neil, Quarmby & Lisa Jane, Young (2010). *Managing intelligence: the art of influence*. Sydney: Federation Press.
20. Van der Beken, T. (2004). Risky business: A risk based methodology to measure organized crime. *Crime Law and Social Change*, 41, 471-516.

DOI: https://doi.org/10.36486/978-966-2310-66-5-13

Я не вірю в невдачі. Немає жодної невдачі, якщо ви отримали насолоду в процесі.

Опра Вінфрі

РОЗДІЛ 13
Процес кримінального аналізу

Олександр Користін
Олександр Виноградов
Владислав Бурангулов

Процес кримінального аналізу, який традиційно називають аналітичним циклом, описує і виділяє шість загальновизнаних, стандартних етапів, які використовуються для перетворення необроблених даних та інформації в аналітичні продукти, що передбачають конкретні дії [1]. Такий підхід відповідає сучасним вимогам розвитку кримінального аналізу, який базується на засадах аналітичної розвідки, – ключового компоненту Intelligence-led Policing.

Процес починається з прийняття рішення або постановки завдання, за яким іде етап планування, після чого аналітики беруть участь у зборі інформації й даних, що підлягають оцінюванню відповідно до офіційно визнаної системи оцінювання (в НПУ оцінка даних та інформації на практиці не використовується).

Наступним кроком є фактичний етап обробки, який починається з зіставлення і структурування доступних даних та інформації й внесення їх у базу даних.

Потім дані й інформація аналізуються, що призводить до отримання аналітичних продуктів для одержувача (керівника, слідчого або інших осіб, які формують завдання для аналітика щодо їх аналізу) та інших відповідних зацікавлених сторін.

Передані аналітичні продукти оцінюються одержувачем з урахуванням потреб і вимог. Зворотний зв'язок використовується для підвищення якості аналітичних продуктів або як методологічна інформація для майбутніх аналогічних аналітичних продуктів.

Аналітичний цикл – це не статична послідовність з шести етапів, а динамічний процес, де різні фази тісно взаємозв'язані та переходять одна в одну, що змушує аналітиків рухатися як уперед, так і назад у межах аналітичного циклу. Цикл, представлений на рис. 13.1, забезпечує структуру та процес, які є впорядкованими та легкими для розуміння, і можуть використовуватися як базовий процес як для стратегічного, оперативного, так і для тактичного аналізу.



Рисунок 13.1. Процес кримінального аналізу

Цикл аналітичної діяльності розпочинається чітким завданням для розробки конкретних аналітичних продуктів. Однак аналітичний процес здійснюється на кількох різних рівнях і часто не обмежується циклом аналітичної діяльності. Цей процес вимагає добре функціонуючої та структурованої організа-

ції роботи з аналітикою на основі визначених стандартів. У країнах ЄС використовуються стандартні операційні процедури (Standard Operating Procedures – SOPs) [1], які дозволяють наповнювати цикл аналітичної діяльності інформацією та визначають очікуваний результат циклу та подальші дії.

ПОСТАНОВКА ЗАВДАНЬ І ПЛАНУВАННЯ

Цикл аналітичної діяльності ініціюється рішенням керівництва, яке визначає аналітикам завдання щодо певної проблеми або напряму. На основі цього завдання керівництво та аналітик обговорюють та узгоджують технічне завдання (ТЗ) – документ, що визначає обсяг, основні цілі, зміст та часові рамки продукту аналітичної діяльності. ТЗ є офіційною відправною точкою циклу аналітичної діяльності.

Важливість чіткого визначення завдань і узгодження цілей продукту аналітичної діяльності часто недооцінюється. Щоб чітко поставити завдання аналітикам, керівники правоохоронних органів й особи, які приймають рішення, повинні знати потенціал та обмеження аналітичного аналізу даних. Подібним чином аналітики повинні знати, як допомогти дослідникам, менеджерам й особам, які приймають рішення (клієнтам), створюючи індивідуальні продукти та цільові рекомендації.

Фаза постановки завдань, яку іноді називають «фазою прийняття рішення», вимагає тісної співпраці між аналітиками та замовниками. Вони повинні *узгодити предмет аналітичної розвідки, цілі, мету, масштаби, часові рамки та форму звітності, включаючи розповсюдження та одержувача аналітичного продукту [1].* Аналітик повинен чітко розуміти очікування та наміри замовника.

Важливо ставитися до таких завдань як до проектів і ретельно планувати різні етапи. Складні проєкти можуть вимагати значної кількості часу та ресурсів. Ґрунтуючись на ТЗ, і відповідно до обсягу проєкту, аналітик повинен розробити детальний план проєкту, який містить узгоджені цілі, обсяг і часові рамки, а також послідовність дій і перелік ресурсів, необхідних для успішного виконання завдання. Цей етап є незамінним, оскільки він слугуватиме керівництвом для збору та подальшого аналізу інформації. План проєкту також повинен враховувати можливі юридичні проблеми та проблеми захисту даних, які можуть виникнути під час реалізації проєкту аналітичної діяльності. Зокрема, якщо йдеться про використання персональних даних або таємних методів збору даних та інформації, правові вимоги та можливі обмеження слід враховувати на ранній стадії процесу планування для забезпечення збору, обміну та використання даних та інформації здійснюється суворо відповідно до національного законодавства та міжнародних стандартів.

Чітке планування економить час у довгостроковій перспективі та забезпечує ефективне використання ресурсів, що призводить до підвищення якості результату. Це також зменшує ризик того, що збір, зберігання, обмін та обробка даних й інформації не відповідатимуть національним та міжнародним правовим стандартам, що ставить під загрозу успіх усього проекту. За наявності відповідних завдань і планування аналітичні продукти можуть допомогти у розробці стратегічних планів для вирішення поточних проблем і підготовки до очікуваних.

ЗБІР ТА ОЦІНКА

Збір інформації для забезпечення аналітичного процесу та виконання визначеного завдання є складним процесом. Завдання у цій сфері не є випадковою справою, а випливають з ролі й значення інформації для всієї службової діяльності. Тому також існує постійна потреба в інформації, без якої неможливо вести ефективну службову діяльність.

Інформація – це елемент знання, що повідомляється, передається комусь за допомогою мови або іншого коду; також це те, що у цій ситуації може надати певне знання (новина, повідомлення, підказка). Можемо розуміти інформацію також як будь-які дані про зовнішній світ, які одержуємо як безпосереднім шляхом, через органи відчуття, так і опосередкованим шляхом, завдяки опису певного стану речей, який наводиться людиною [2]. Особливого значення у реалізації майбутніх службових дій набирає корисна інформація, тобто:

відповідна *– спрямована на виконання завдань правоохоронної діяльності, які передбачені законодавством та інтересів, що випливають з цих завдань;*

точна *– яка достовірно відображає дійсність;*

повна *– що надає всі необхідні дані;*

своєчасна *– доступна у той час, який уможливлює її належне використання.*

Виділяють такі способи збору інформації [3]:

Спостереження *– спосіб дослідження, який полягає в навмисному, систематичному і цілеспрямованому сприйнятті об'єктів, явищ із метою вивчення їх специфічних змін у певних умовах і відшукуванні смислу цих явищ.*

Опитування *як спосіб збору інформації передбачає її збирання шляхом реєстрації показників від осіб, яких опитують.*

> *Експертне опитування, як різновид, є важливим елементом збору інформації для забезпечення прогностичних аналітичних завдань, оцінки ризиків тощо.*

Фотофіксація *застосовується в процесах, що відбуваються у практичній сфері. Їх поділяють на такі різновиди: фотографія підозрілих осіб, фотографія часу та місця події, маршрутна фотографія, самофотографія.*

Опис *– спосіб дослідження, який полягає в зазначенні ознак об'єкта. Це може бути усне або письмове визначення кількісних чи якісних ознак, властивостей у певній послідовності.*

Хоча аналітики повинні забезпечити активний пошук достатньої кількості даних, щоб охопити всі аспекти, що підлягають аналізу, вони повинні уникати перевантаження даними та збору непотрібної або неадекватної інформації.

> *Ключовим питанням щодо обігу й службового використання інформації є уміння правильно її оцінити.*

Для досягнення цієї мети необхідним є знання сутності інформації, видів джерел інформації, а також знання специфіки її передачі та принципи управління інформацією.

Ключовим етапу збору даних та інформації є знання щодо існування, актуальності, доступності та надійності усіх джерел, обраних для виконання конкретного завдання збору, а також вимог щодо повноважень використання даних та інформації з різних типів джерел інформації.

> *Знання та доступ до внутрішніх і зовнішніх даних та джерел інформації, а також поінформованість про потенційні обмеження та вимоги є передумовами для ефективного збору, забезпечуючи його розвідувальний характер, та подальшого успішного аналізу [1].*

Розробка плану збору є наступним кроком після узгодження ТЗ і плану проекту. План збору є обов'язковим для забезпечення впорядкованого та точного збору відповідних даних та інформації для забезпечення запитуваних/визначених вимог [1]. Це слід розглядати як безперервний процес із можливістю адаптації та реагування на зміни вимог. План збору базується на визначенні поняття, об'єкту, обсягу й термінів виконання завдання та описує:

- ***яка*** *інформація повинна бути зібрана або є у розпорядженні, включаючи мету та цінність даних;*
- ***які*** *джерела слід використовувати;*
- ***де*** *можна отримати інформацію;*
- ***як*** *можна отримати інформацію*
- ***хто*** *повинен її збирати;*
- ***скільки*** *даних можна обробити;*
- ***коли*** *потрібно збирати кожен фрагмент даних.*

У деяких випадках може виникнути потреба включити пояснення, чому необхідно збирати певні дані та інформацію. Як загальний план проєкту, план збору також повинен враховувати різні законодавчі вимоги, які застосовуватимуться до завдань збору залежно від типу інформації, яку потрібно зібрати, а також джерел і засобів, які використовуються для її отримання [4].

Розробка детального плану збору, який включає оцінку потреб і необхідні юридичні дозволи, а також вимоги щодо нагляду, які можуть застосовуватися, має важливе значення для успіху проєкту. Таким чином, план забезпечить дотримання всіма залученими сторонами узгоджених цілей і відповідних стандартів.

Системи оцінювання даних. Одночасно або відразу після збору інформації, отримані дані потрібно оцінити у контексті, в якому вони були отримані [1]. Оцінювання даних має ґрунтуватися на об'єктивному професійному судженні, оскільки якість даних визначає достовірність розробленої аналітики. Під час оцінки враховується достовірність і надійність інформації та її корисність для виконання завдання [2; 3; 5]. Загальним першим кроком є визначення того, що є важливим, а що несуттєвим, а також оцінювання нагальності подальших дій на основі отриманої інформації.

> *Надійність джерела, достовірність та точність інформації повинні оцінюватися окремо співробітником/аналітиком, який отримав і зареєстрував цю конкретну інформацію [6].*

Усі джерела та всю інформацію слід оцінювати відповідно до офіційно визнаної системи оцінювання [1]. І хоча в Україні, зокрема і в Національній поліції, сьогодні не унормовано процес оцінювання інформації,

розглядаючи його як обов'язковий атрибут сучасної правоохоронної системи та об'єктивність упровадження у майбутньому, важливо розуміти змістовні особливості процесу, ключові аспекти та вимоги.

Метою оцінки інформації є:
- ✓ *уніфікація інтерпретації інформації всіма її користувачами;*
- ✓ *зменшення ризику під час прийняття рішень;*
- ✓ *точніше прогнозування розвитку ситуації;*
- ✓ *підготовка вичерпних версій в оперативно-слідчій діяльності;*
- ✓ *прийняття адекватних та оптимальних рішень;*
- ✓ *мінімізація витрат на заходи, що проводяться.*

Результатом оцінки інформації повинен стати висновок щодо її релевантності для досліджуваного предмету.

Релевантність інформації *– наявність зв'язку з проблемою (відповідність нашим інтересам) і здатність інформації внести вклад в процес розуміння проблеми [3].*

Для того, щоб в подальшому досить ефективно працювати з інформацією (використовувати її), потрібно на початковому етапі зрозуміти:
- ✓ *корисна для вас викладена інформація чи ні,*
- ✓ *чи можна їй довіряти,*
- ✓ *чи потрібна додаткова інформація тощо.*

Головною метою оцінки інформації є використання загальноприйнятих знаків (індексів) надійності джерела й достовірності змісту інформації, що має критично важливе значення для аналітичного процесу та формування висновку.

З погляду оцінки важливості інформації, важливим питанням є поняття «джерела». *Джерелом інформації є об'єкт (особа, річ тощо), що спроможний зберігати набуту інформацію безпосередньо або опосередковано, і який можна використати для її прийому*. Джерело – це початок чогось, причина певних подій, це матеріали, які надають дані, що становлять основу для подальших досліджень.

Кожне джерело інформації є різним і має розглядатися індивідуально. Оцінюючи характеристики джерела, особа, що його оцінює, завжди зобов'язана дати собі відповідь на кілька запитань, зокрема:

До якої групи належить це джерело?

Яку воно має мету, передаючи інформацію?

Чому співпрацює (свідомо чи несвідомо, добровільно чи, наприклад, під правовим примусом)?

Це, безумовно, найважливіший елемент верифікації (перевірки) особливо власних джерел, оскільки вони найчастіше можуть створювати загрозу свідомих дій, спрямованих на дезінформацію.

Крім того, оцінка характеристики особистого джерела охоплює також визначення й безперервну модифікацію знання посадової особи про можливості джерела, його інтелектуальний рівень, індивідуальні риси тощо. Дуже часто, наприклад, різноманітні бази даних – також по причині умисних (або випадкових) дій осіб – можуть бути «підозрілими», і внаслідок цього отримати різну оцінку. Таким чином, ***належна оцінка вимагає*** *оцінки надійності джерела інформації та оцінки достовірності її змісту, які здійснюються незалежно.*

Надійність джерела інформації оцінюється за такими критеріями:

A *(абсолютно надійне) – немає сумнівів щодо автентичності, достовірності та обізнаності джерела або якщо інформація походить із джерела, яке в минулому завжди виявлялося достовірним;*

B *(надійне в більшості випадків) – незначні сумніви про автентичність, надійність або компетентність джерела, з якого отримувана інформація переважно виявлялася достовірною;*

C *(у більшості випадків не надійне) – джерело, з якого отримувана інформація у більшості випадків, виявлялась недостовірною, у минулому частина інформації була надійною;*

D *– визначити надійність немає можливості.*

За критерієм надійності «А» джерелами інформації є:
- *технічні засоби, за допомогою яких проводилася безпосередньо фіксація відео-, аудіо- або іншої інформації, що може бути перевірено та підтверджено уповноваженою особою, що проводить оцінку надійності джерела;*
- *об'єкти та їх сліди, отримані в результаті використання спеціальних знань, виявлення, фіксація, вилучення та дослідження яких було здійснено відповідно до чинного законодавства;*
- *банки та бази даних державних та міжнародних установ та організацій;*
- *фахівець – особа, яка володіє науковими, технічними або іншими спеціальними знаннями та має документи відповідного державного або міжнародного зразка;*

- державні установи, підприємства та організації, які надають інформацію за встановленою формою державного зразка;
- офіційні державні засоби масової інформації України та інших країн.

За критерієм надійності «B» джерелами інформації є:
- будь-які технічні засоби (мобільні телефони, комп'ютери, системи відеоспостереження, ігрові консолі, обладнання для зв'язку, обладнання для запису інформації тощо);
- недержавні, комерційні установи, підприємства та організації, до сфери діяльності яких належить інформація, що надається, та які в минулому в більшості випадків виявилися надійними джерелами (3 та більше разів та були оцінені за рівнем надійності не нижче «B»);
- громадяни України, іноземні особи та особи без громадянства, особистості яких встановлені та які в минулому в більшості випадків виявилися надійними джерелами (3 та більше разів та були оцінені за рівнем надійності не нижче «B»).

За критерієм надійності «C» джерелами інформації є:
- громадяни України, іноземні особи та особи без громадянства, особистості яких встановлені, які в минулому були як надійними (менше 3-х разів та були оцінені за рівнем надійності не нижче «B) так і ненадійними джерелами (достатньо 1-го разу);
- громадяни України, іноземні особи та особи без громадянства, особистості яких встановлені, які мають особисту зацікавленість в наданні інформації;
- недержавні, комерційні установи, підприємства та організації, до сфери діяльності яких належить інформація, що надається, та які в минулому були як надійними (менше 3-х разів та були оцінені за рівнем надійності не нижче «B») так і ненадійними джерелами (достатньо 1-го разу).

За критерієм надійності «D» джерелами інформації є:
- будь-які невстановлені особи;
- недержавні засоби масової інформації;
- будь-яка особа, установа, підприємство чи організація, яка не може бути оцінена за рівнем надійності «A», «B», «C».

Оцінка достовірності змісту інформації здійснюється за такими критеріями:

***1** (інформація повністю достовірна) – інформація, точність якої не підлягає сумніву, підтверджена іншими незалежними джерелами; логічна за своєю суттю; відповідає іншій інформації з цього питання;*

***2** (інформація відома джерелу особисто) – інформація, відома особисто джерелу, але не відома особисто співробітнику, який її приймає і передає далі, не підтверджена, логічна за своєю суттю, відповідає іншій інформації з цього питання;*

***3** (інформація джерелу особисто невідома, але підтверджується іншою інформацією) – інформація, невідома особисто джерелу, однак підтверджена іншою, вже зібраною інформацією, достатньо логічна за своєю суттю;*

***4** (інформація джерелу невідома, і підтвердити її немає можливості) – інформація, невідома особисто джерелу і яку неможливо підтвердити, можлива, але нелогічна, не є достовірною на момент отримання, але вірогідність не виключається.*

За критерієм достовірності інформації «1» інформація, яка:
- підтверджена та взаємопов'язана з іншою інформацією (кількість інформаційних даних повинна бути 3 та більше, водночас інформаційні дані повинні бути за рівнем достовірності не нижче «2», а джерела цих інформаційних даних незалежні один від одного – не нижче рівня надійності «B»);
- крім свого джерела має ще не менше 3-х незалежних джерел з рівнем надійності не нижче «B»;
- перевірена та підтверджена особою, яка проводить оцінювання достовірності інформації.

За критерієм достовірності інформації «2»:
- підтверджена та взаємопов'язана з іншою інформацією (кількість інформаційних даних повинна бути 2, водночас інформаційні дані повинні бути за рівнем достовірності не нижче «2», а джерела цих інформаційних даних незалежні один від одного – не нижче рівня надійності «B»);
- крім свого джерела має ще не менше 2-х незалежних джерел з рівнем надійності не нижче «B»;
- відома джерелу особисто, хоча особа, яка оцінює вказану інформацію особисто її не сприймала.

За критерієм достовірності інформації «3»:
- підтверджена та взаємопов'язана з іншою інформацією (кількість інформаційних даних повинна бути 1, водночас інформаційні дані повинні бути за рівнем достовірності не нижче «2», а джерела цих інформаційних даних незалежними один від одного та не нижче рівня «B») або підтверджена та взаємопов'язана з іншою інформацією (кількість інформаційних даних повинна бути 2, вод-

ночас рівень достовірності цих інформаційних даних повинен бути не нижче «3», а джерела цих інформаційних даних незалежні один від одного – не нижче рівня надійності «С»);
- *крім свого джерела має ще не менше 1-го незалежного джерела з рівнем надійності не нижче «В» або, крім свого джерела, має ще не менше 2-х незалежних джерел з рівнем надійності не нижче «С»;*
- *може бути отримана джерелом від третьої сторони, в тому числі й з засобів масової інформації.*

За критерієм достовірності інформації «4»:
- *не підтверджена іншою інформацією;*
- *немає незалежних джерел, які підтверджують зазначену інформацію;*
- *має у своєму змісті суперечливі судження або нелогічна.*

Розглядаючи співвідношення джерела й інформації, як основний критерій оцінки, потрібно обов'язково врахувати обставини, за яких джерело отримало передану потім інформацію: чи воно було наочним свідком події, чи також передане знання отримано опосередковано (а якщо так, то в який спосіб, від кого, за яких обставин), чи є вичерпною інформація, що передається, чи, наприклад, вона є частковою і чому так сталося, чи існує ймовірність того, що це джерело взагалі могло отримати таку інформацію.

> *Присвоєння коду **достовірності інформації** – це встановлення співвідношення джерела й інформації – визначення того, яким чином джерело стало власником інформації, яку воно передає. Виконання цієї оцінки неможливе без попередньої оцінки самого джерела (як його характеристики, так і його достовірності).*

Визначаючи коди достовірності змісту інформації, службова особа суб'єктивно оцінює ***достовірність, а не правдивість*** змісту отриманої інформації.

У посібнику ОБСЄ «Guidebook Intelligence-led Policing» [1] наводяться приклади визначення кодів оцінки за системою 4х4 та 5х5х5 (табл. 13.1, 13.2).

Заключним етапом є прийняття обґрунтованого рішення щодо достовірності інформації, яке випливає з аналізу джерела та інформації.

На цьому етапі уповноваженою особою проводиться певний підсумок, який ґрунтується на оцінці надійності джерела та достовірності інформації.

Таблиця 13.1., 13.2. Коди оцінювання за системою оцінювання 4х4 та 5х5х5

ОЦІНКА ДЖЕРЕЛА		ОЦІНКА ІНФОРМАЦІЇ	
A	Повністю надійне у всіх випадках	1	Точність не викликає сумнівів
B	Зазвичай надійне	2	Особисто відома джерелу, але не відома особисто офіційній особі, яка її передає
C	Зазвичай ненадійне	3	Особисто невідома джерелу, але підтверджується іншою доступною інформацією
D	Надійність неможливо оцінити	4	Точність неможливо оцінити або підтвердити будь-яким способом (наразі)

ОЦІНКА ДЖЕРЕЛА		ОЦІНКА ІНФОРМАЦІЇ	
A	Завжди надійне	1	Відомо, що беззастережно вірна
B	Переважно надійне	2	Відома особисто джерелу, але не особі, яка повідомляє
C	Іноді надійне	3	Невідома особисто джерелу, але підтверджена
D	Ненадійне	4	Неможливо оцінити
E	Неперевірене джерело	5	Підозра на неправдивість

Кодування достовірності інформації відповідно до критеріїв оцінки надійності джерела інформації («А», «В», «С», «D») та достовірності самої інформації («1», «2», «3», «4»).

Присвоєння коду достовірності інформації – це ніщо інше, як встановлення співвідношення джерела й інформації – визначення того, яким чином джерело стало власником (особою, що володіє) інформації, яку воно передає. Проте виконання цієї оцінки неможливе, про що вже згадувалося раніше, без попередньої оцінки самого джерела (як його характеристики, так і його достовірності) і з цією оцінкою воно тісно пов'язане. Найбільш часто застосовуваними системами оцінки є: **4х4, 5х5, 5х5х5, 6х6.**

Таким чином, загальний процес оцінки є дослідженням ступенів ***надійності джерела та достовірності змісту інформації***. Наприклад, у системі оцінки 4х4 використовуються чотири ступені оцінки надійності джерела інформації та чотири ступені оцінки достовірності змісту самої інфор-

мації, у системах 5x5 та 6x6 таких критеріїв відповідно п'ять та шість. В окремих випадках у бланки оцінки потрібно вносити інформацію про ступінь поширення (доступу) відповідної інформації, так звані «коди обробки» (5x5x5).

За потреби інформація може бути з легкістю конвертована з однієї системи в іншу. Але найбільш розповсюдженою системою оцінки інформації є 4x4, яка дає змогу отримання 16 різних оцінок у діапазоні від A1 до D4.

Аналізуючи інформацію на тлі оцінки її достовірності, прийнято твердження, що інформація, достовірність якої оцінено на рівні A1, A2, B1 або B2, є достовірною інформацією – і у зв'язку з цим немає необхідності її підтвердження (хоча вибірково це робити потрібно). Але інші класифікації – від B3 до D4 інтерпретуються як недостовірна інформація, яка, особливо під час аналітичної діяльності, і не тільки, потребує додаткового підтвердження і перевірки.

Правило: у *випадку сумнівів надається нижча оцінка* – ***краще недооцінити, ніж переоцінити!***

Оцінка актуальності, надійності та точності інформації, а також визначення коду обробки для її подальшого використання є важливими для точності остаточного аналітичного продукту та умов їх поширення. Таким чином, узагальнюючи викладене, важливо враховувати загальний алгоритм оцінки інформації та проводити її за такими етапами:

1) складання характеристики джерела інформації;
2) оцінка надійності джерела інформації;
3) аналіз інформації;
4) оцінка достовірності змісту інформації;
5) оцінка співвідношення джерела та інформації;
6) прийняття обґрунтованого рішення щодо достовірності інформації;
7) кодування достовірності інформації;
8) фільтрація змісту інформації;
9) формалізація оцінки достовірності інформації.

Але оцінка також важлива з точки зору прав людини та захисту даних. Стандарти захисту даних вимагають, серед іншого, щоб збережена особиста інформація була точною, адекватною, актуальною та не була надмірною щодо мети, для якої вона зберігається. Таким чином, оцінка має ключове значення для доказу того, що реєстрація інформації, яка є втручанням у право на недоторканність особистих даних/суб'єкта інформації, є обґрунтованою, необхідною та пропорційною, і отже, допустимою, відповідно до чинних стандартів прав людини та захисту даних [1].

Ті хто здійснюють оцінку також повинні усвідомлювати інші можливі проблеми з правами людини, які можуть мати відношення до того, як певна інформація може використовуватися. Це особливо важливо під час оцінки інформації з третіх країн, якщо є підстави вважати, що інформація могла бути отримана незаконним шляхом. Використання доказів, отриманих шляхом тортур та інших жорстоких дій, у судовому процесі, наприклад, абсолютно заборонено міжнародним правом. Але навіть якщо інформація або дані, отримані таким чином, не призначалися для використання у судових процесах, вони не вважаються прийнятними у будь-якому випадку [4].

Загальним підсумком є дотримання таких правил здійснення оцінки інформації:

1. *Особа, яка буде проводити діяльність з оцінки надійності джерела і достовірності змісту інформації повинна опанувати значення шкали надійності джерела та шкали достовірності інформації.*
2. *Під час оцінки надійності джерела аналізу піддається: характеристика джерела, надійність джерела та відношення змісту даних до джерела.*
3. *Під час оцінки надійності та достовірності змісту інформації аналізу піддається: достовірність даних, та те, чи підтверджується інформація іншими даними.*
4. *Особа, яка проводить оцінку даних використовує засоби оцінки джерела та змісту інформації, використовуючи знаки надійності.*

ЗВЕДЕННЯ ТА ОБРОБКА

Етап обробки та зведення вимагає наявності адекватної та узгодженої системи. Ця фаза передбачає сортування, визначення пріоритетів та посилання на зібрану інформацію. На етапі зведення аналітик упорядковує та структурує зібрану інформацію, перетворюючи її на індексований формат із перехресними посиланнями та поміщає її до системи зберігання (тобто базу даних). Перевірка актуальності, точності та корисності інформації є важливим кроком перед тим, як додати її до системи зберігання. Наявність доступної системи, з якої можна отримати та проаналізувати інформацію є важливою особливістю.

Обробка інформації може бути настільки тісно пов'язана з аналітичною фазою, що складно провести між ними чітке розділення [5].

Наприклад, загальною методологічною вимогою Data Sience є обов'язковість проведення очищення даних перед початком їх аналізу, особливо коли мова йде про Big Data. Водночас правоохоронні методології все частіше звертаються до джерел інформації, які продукують великі дані: OSINT, опитування експертів, соціологічне дослідження тощо.

Очищення даних та визначення надійної вибірки. Сучасні правоохоронні політики у розвинених безпекових системах переважно базуються на засадах формування адекватних знань щодо системних кримінальних явищ, кримінального середовища та розбудови відповідних стратегій. Поряд з тим, латентна злочинність, зокрема економічна, а також організовані її прояви, а в Україні ще й невідповідність офіційної кримінальної статистики щодо рівня криміногенних ризиків у суспільстві [7; 8], спонукають до пошуку нових форм аналізу злочинності. Прикладами таких підходів є методологія Європолу SOCTA [9] та ризик-орієнтовані правоохоронні стратегії [10; 11], що базуються на експертних опитуваннях та застосуванні відповідних соціологічних й статистичних методів аналізу.

Збір даних з використанням онлайнових опитувань стає все більш розповсюдженим засобом отримання інформації від респондентів, зважаючи на можливість швидко дізнатися думку великої кількості людей, до яких проблематично дістатися, по великій кількості питань. Проте якість зібраних даних таких опитувань може суттєво страждати через недостатню компетентність експертів, знижену мотивацію надавати продумані відповіді, втому й неуважність внаслідок надмірної кількості й складності питань та дії відволікаючих факторів, установочної поведінки, якості інструментарію й технічних моментів реалізації опитування.

Для контролю установочних стилів й уважності під час заповнення запитальників дослідники зазвичай включають в анкету спеціально створені контрольні питання [12]:

- *для вимірювання соціальної бажаності відповідей;*
- *однакові за змістом питання із прямим і зворотним ключем;*
- *питання для перевірки компетентностей респондентів;*
- *прямі інструкції (наприклад: «На це питання оберіть відповідь 2»).*

Якщо перед проведенням опитування подібні інструменти не були заплановані, доводиться ідентифікувати неуважних, некомпетентних чи невмотивованих респондентів в інший спосіб, спираючись на статистичні властивості їхніх відповідей.

Такими ознаками низької якості даних у конкретного респондента можуть виступати [13]:

- *значна кількість пропусків;*
- *надто короткий час реагування на питання;*
- *низька варіативність відповідей на низку питань;*
- *наявність невипадкових патернів відповіді на низку питань, які не визначаються їхнім змістом;*
- *суттєва відмінність відповідей респондента від профілю відповідей значної маси добросовісних і компетентних учасників.*

ПРАКТИЧНИЙ КЕЙС

з очищення даних та визначення надійної вибірки

На основі соціального опитування, за участі усіх суб'єктів фіскальної безпеки в Україні було започатковано аналіз стратегічного рівня, окремими питаннями якого визначено оцінку ризиків цілеспрямованої діяльності організованої злочинності у сфері фіскальної безпеки України. На основі унікальної емпіричної бази, сформованої опитуванням суб'єктів фіскальної безпеки України [11], було також визначено аналітичне завдання щодо очищення даних генеральної експертної сукупності, формування надійної експертної вибірки [12] та забезпечення достатньої репрезентативності аналітичних висновків.

Уже початкові аналітичні висновки, проведення стратегічного аналізу у сфері фіскальної безпеки України на основі ризик-орієнтованого підходу, акцентували увагу на надзвичайній важливості такої новації та сформували систему знань щодо обґрунтування пріоритетних напрямів подальшого розвитку зазначеного сегменту.

> *Використовуючи методологію ризик-менеджменту було ідентифіковано та оцінено загрози у сфері фіскальної безпеки (243), проведено аналіз та оцінювання ризиків їх поширення, визначено граничні розміри ризиків, оцінено спроможності (119) й зовнішні можливості (52) мінімізації ризиків, а також спроєктовано прогнозну модель з управління зазначеними ризиками [11].*

Водночас важливо зазначити, що отримані висновки потребують достатнього рівня об'єктивності, надійності та репрезентативності даних. Саме тому було використано декілька способів очищення зібраного масиву даних.

В основі нашої гіпотези покладено припущення щодо недостатньої надійності отриманих даних під час опитування більше 7 тисяч респондентів (експертів у сфері фіскальної безпеки). Таке припущення

мотивувалося вже тим, що опитуваним необхідно було в режимі он-лайн без зовнішнього нагляду заповнити опитувальник у два етапи та оцінити за подвійною шкалою «ймовірність» і «наслідки» більше 400 індикаторів [11], що характеризували загрози, спроможності (вразливості) та зовнішні можливості. Звісно, таке завдання є складним і не всі респонденти могли приділити достатню увагу заповненню опитувальника. Статистичні обґрунтування процедури обмеження вибірки базуються на тому, що через значний обсяг анкети експерти могли припускатися помилки у відповідях, оскільки складність питань й обмежений час їх осмислення призводить до нестійкості уваги.

> *З метою перевірки гіпотези та забезпечення ймовірного очищення даних, перш за все, було використано метод логічної помилки (фільтр 1).*

Зокрема, окремі індикатори в різних розділах опитувальника використано для перевірки компетентності респондентів.

Наприклад, *за індикатором «Рівень тіньової економіки», логічно обґрунтованою відповіддю під час оцінювання ймовірності поширення цієї загрози за шкалою «низька-середня-висока» можливою є «середня» або «висока» ймовірність, але не компетентною буде вважатися відповідь «низька ймовірність» щодо рівня тіньової економіки в Україні.*

Використовуючи зазначений індикатор як фільтр, було зроблено першу вибірку з масиву даних генеральної сукупності чим суттєво підвищено якість даних для подальшого аналізу. Це можна бачити на такому прикладі: *рівень ризику поширення загрози за індикатором TA2 (цілеспрямована діяльність організованих злочинних угруповань щодо ПДВ), яке належить до найбільших загроз, мають наступні розподіли у групі тих, хто був відібраний за фільтром відсутності логічних помилок, у порівнянні з тими, хто цей фільтр не пройшов (табл. 13.3).*

Таблиця 13.3. Порівняння надійної та ненадійної вибірок після застосування Фільтру 1

	Рівень оцінки	Ненадійна вибірка	Надійна вибірка	Всього
TA2 – цілеспрямована діяльність організованих злочинних угруповань щодо ПДВ	*низький*	16.7%	2.2%	11.5%
	середній	43.2%	17.8%	34.1%
	високий	40.1%	80.0%	54.4%
Всього	**100.0%**		**100.0%**	**100.0%**

Різниця в розподілах є значною: 16,7% ненадійних експертів вказали на низьку ймовірність прояву загрози, в той час як надійні обрали цей варіант лише у 2,2% випадків. Варіант «висока ймовірність» був обраний ними у 80% випадків. Ця різниця є не тільки статистично значущою (критерій χ^2 = 38.378, p < 0.001), але й величина ефекту є дуже значною (V Крамера = 0.39). Аналогічні тенденції спостерігаються і по інших важливих питаннях анкети.

Для підвищення якості відібраних даних, що є достатньо обґрунтованим припущенням,

> *використано додатково метод (фільтр 2), що базується на виявленні патернів (профілів) відповіді респондентів на питання з наступним визначенням якості інформації в профілі*

на основі варіативності відповідей, частки пропущених даних і осмисленості відповідей (зазначене визначається окремо). Для ідентифікації груп респондентів із різним стилем реагування на низку питань

> *використано такий алгоритм, який у своїй основі базується на кластерному аналізі методом K середніх.*

Якість наданої респондентом інформації визначається окремо по обраному блоку питань, а не анкеті в цілому. Аналізу були піддані 35 індикаторів (TA2–TA36), що характеризують рівень ризику поширення загроз, пов'язаних з цілеспрямованою діяльністю організованої злочинності у сфері фіскальної безпеки. Такий підхід дає можливість зберегти максимум експертної інформації, оскільки виходить з припущення, що уважність, компетентність і вмотивованість експерта можуть варіювати у часі або залежати від змісту питань в блоці. Також зазначимо, що рівень ризику визначається на основі інтегральної оцінки ймовірності і наслідків визначених загроз.

> *Статистичний аналіз даних здійснювався за допомогою пакету IBM SPSS Statistics версії 25, проте запропонований алгоритм легко реалізувати з використанням мови R [14].*

Наступним кроком у алгоритмі є заповнення пропущених відповідей. Необхідно зазначити, що значна кількість пропущених даних є суттєвою проблемою у разі проведення будь-якого статис-

тичного аналізу, тому пропуски (в цьому випадку це код 99) замінювалися нами на значення, близьке до модальної відповіді (наприклад 10), але трохи відмінне від неї (наприклад 9) для полегшення інтерпретації кластерів (рис. 13.2).

```
FREQUENCIES
VARIABLES=TA2 to TA36
/FORMAT=NOTABLE
/STATISTICS=MEAN MEDIAN
/ORDER=ANALYSIS.

RECODE TA2 (MISSING = 25).
RECODE TA3 (MISSING = 25).
RECODE TA4 (MISSING = 25).
RECODE TA5 (MISSING = 15).
RECODE TA6 (MISSING = 25).
RECODE TA7 (MISSING = 10).
RECODE TA8 (MISSING = 15).
RECODE TA9 (MISSING = 15).
RECODE TA10 (MISSING = 15).
RECODE TA11 (MISSING = 15).
RECODE TA12 (MISSING = 15).
RECODE TA13 (MISSING = 30).
RECODE TA14 (MISSING = 30).
RECODE TA15 (MISSING = 30).
RECODE TA16 (MISSING = 30).
RECODE TA17 (MISSING = 30).
RECODE TA18 (MISSING = 30).
RECODE TA19 (MISSING = 30).
RECODE TA20 (MISSING = 25).
RECODE TA21 (MISSING = 30).
RECODE TA22 (MISSING = 30).
RECODE TA23 (MISSING = 30).
RECODE TA24 (MISSING = 30).
RECODE TA25 (MISSING = 30).
RECODE TA26 (MISSING = 30).
RECODE TA27 (MISSING = 30).
RECODE TA28 (MISSING = 15).
RECODE TA29 (MISSING = 30).
RECODE TA30 (MISSING = 30).
RECODE TA31 (MISSING = 15).
RECODE TA32 (MISSING = 15).
RECODE TA33 (MISSING = 30).
RECODE TA34 (MISSING = 15).
RECODE TA35 (MISSING = 15).
RECODE TA36 (MISSING = 15).
execute.
```

Рисунок 13.2. Синтаксис IBM SPSS Statistics для визначення медіани та заміщення пропущених даних

Це дозволило ідентифікувати відсутність відповідей у патерні. *На наступному кроці здійснюється кластерний аналіз масиву даних по обраному блоку питань одним з обраних алгоритмів (Two Step Cluster Analysis, K-Means Clustering). Експерименти показали, що найбільш зручним у використанні виявився метод К-середніх.*

Важливо зазначити, що результати кластеризації завжди є дещо нестійкими і залежать від того, за якими змінними був відсортований масив. Тому процедуру розбиття на кластери варто повторити декілька разів, попередньо сортуючи масив за різними змінними й перевіряючи стабільність рішення.

Важливими моментами під час проведення кластеризації є вибір кількості кластерів, на які розбивається вся сукупність. На початковому етапі, зважаючи на загальний об'єм вибірки експертів, нами виділялося 10 кластерів (рис. 13.3).

```
QUICK CLUSTER TA2 TO TA36
  /MISSING = LISTWISE
  /CRITERIA = CLUSTER(10) MXITER(999) CONVERGE(0)
  /METHOD = KMEANS(NOUPDATE)
  /PRINT INITIAL.
```

Рисунок 13.3. Синтаксис кластерного аналізу за методом К Середніх

Таблиця 13.4. Описові статистики

№ кластера	Мінімум	Максимум	Середнє	Станд. відх-ня
K1 - 35	70.15	89.70	81.3793	4.75563
K2 - 35	26.12	70.58	46.9253	13.27791
K3 - 35	18.75	35.42	26.2580	4.93323

Водночас частина кластерів виявилися мало наповненими та дещо подібними, що свідчить про необхідність поступового зменшення їхньої кількості до оптимальної. У нашій вибірці даних оптимальним є вибір трьох кластерів (табл. 13.4).

У результаті кластеризації в основному масиві зберігаються змінні належності респондента до кластеру й відстані до його центру.

Після дослідження варіативності й осмисленості кластерів нами виділено кластер К2, варіативність рівня ризиків за яким оцінюється від min – 26,12 % до max – 70,58 %.

У подальшому нами сформовано нову змінну у масиві даних «QCL_1» та на основі використання фільтру за кластером К2 вибірку даних обмежено з метою її покращення (табл. 13.5).

Таблиця 13.5. Вибірка за кластером К2 після застосування Фільтра 2

	Кластер	Ненадійна вибірка	Надійна вибірка	Всього
QCL_1	K1	17.0%	-	11.2%
	K2	-	100.0%	34.3%
	K3	83.0%	-	54.5%
Всього		**100.0%**	**100.0%**	**100.0%**

Таким чином, лише 34,3 % даних потрапили до вибірки обмеженої фільтром визначеного кластеру К2. Таке обмеження є не тільки статистично значущим (критерій $\chi^2 = 268.000$, $p < 0.000$), але й величина ефекту є дуже значною (V Крамера = 1.0).

Зазначені висновки підтверджують висунуту нами гіпотезу щодо неякісних даних загальної сукупності проведеного опитування у сфері фіскальної безпеки України.

Таким чином, використано алгоритм очищення даних загальної експертної сукупності на основі:

- *перевірки компетентності респондентів;*

- виявлення патернів (профілів) відповідей респондентів на питання з наступним визначенням якості інформації в профілі на основі варіативності відповідей, частки пропущених даних і осмисленості відповідей.

Подальше застосування визначених фільтрів обмеження вибірки надає можливість остаточно оцінити ризики за 35 індикаторами загроз поширення організованої злочинності у сфері фіскальної безпеки України (табл. 13.6).

Таблиця 13.6. Оцінка ризиків цілеспрямованої діяльності оргзлочинності в сфері фіскальної безпеки України

ЗМІННА	ОЦІНКА РИЗИКІВ, %		
	БЕЗ ФІТРІВ	ФІЛЬТР 1	ФІЛЬТР 1,2
TA2	48.54	55.62	**68.91**
TA3	35.57	46.16	54.27
TA4	40.53	50.70	59.96
TA5	32.1	42.42	46.86
TA6	40.91	50.17	56.32
TA7	31.10	39.45	38.22
TA8	28.53	37.21	35.21
TA9	30.23	36.21	32.63
TA10	29.07	34.34	29.20
TA11	30.97	37.78	35.72
TA12	29.62	37.91	34.64
TA13	39.18	46.67	54.09
TA14	36.98	44.48	51.33
TA15	46.83	48.44	55.63
TA16	49.62	51.30	**63.33**
TA17	48.04	52.60	**66.28**
TA18	41.44	49.48	**62.72**
TA19	47.98	49.27	55.31
TA20	35.27	36.97	37.01
TA21	42.02	52.82	**65.08**
TA22	47.34	55.59	**70.58**
TA23	39.73	45.11	49.28
TA24	37.10	42.85	46.28
TA25	45.92	47.42	53.79
TA26	35.53	42.01	43.07
TA27	42.54	50.53	59.32
TA28	33.79	41.01	39.84
TA29	35.18	40.92	42.00
TA30	37.55	44.07	51.44
TA31	31.49	34.96	29.15
TA32	30.51	34.28	28.80
TA33	37.70	40.56	43.03
TA34	28.07	32.36	26.12
TA35	27.26	34.38	30.11
TA36	28.27	36.34	26.86

Остаточна вибірка даних на основі оцінювання ризиків визначає чотири групи загроз поширення цілеспрямованої діяльності організованої злочинності у сфері фіскальної безпеки, з яких:

- *найзначніші* з них (TA2, TA16, TA17, TA18, TA21, TA22) – *червоний* рівень ризику;

- *значні* (TA3, TA4, TA6, TA13, TA14, TA15, TA19, TA25, TA27, TA30) – *оранжевий* рівень ризику.

АНАЛІЗ

Надійність та масштаби аналізу значною мірою залежать від якості та точності попередньо зібраних даних, з одного боку, а також кваліфікації аналітиків, з іншого боку. Під час аналізу інформації, а також на всіх інших етапах аналітичного циклу, тісна співпраця між аналітиками та замовниками (детективами, слідчими, керівництвом), включаючи організацію регулярних оглядових зустрічей, є абсолютно необхідною для забезпечення того, щоб аналіз здійснювався відповідно до розвідувальних потреб та/або вимог замовника.

> *Етап **аналізу** є центральним в аналітичному процесі, оскільки це стосується ідентифікації та з'ясування сутності, контексту й істотних ознак наявної інформації.*

Аналіз даних дозволяє звернути увагу на недостатність інформації, сильні й слабкі сторони даних і визначає напрям наступних кроків. Основною метою на етапі аналізу є отримання сенсу з первинної інформації та можливості подальшого використання аналітичного продукту на практиці.

Аналітичний процес під час аналізу даних складається з двох етапів: *інтеграції даних* та *інтерпретації даних* [1].

Перший етап (інтеграція даних) об'єднує оцінену та зібрану інформацію з різних джерел з метою розробки початкових гіпотез та прогнозів, виявлення патернів та формування узагальнень.

Другий етап (інтерпретація даних) передбачає вихід за межі наявних даних та їх інтерпретацію. На цьому етапі початкові гіпотези перевіряються, в результаті чого підтверджуються, змінюються або спростовуються раніше розроблені гіпотези.

> *Гіпотеза – це попередня робоча теорія, яка базується на раніше розроблених індикаторах і припущеннях, що випливає з наявних даних і яка потребує додаткової інформації, з метою підтвердження або спростування попередніх припущень аналітики та сформованих узагальнень [1].*

Гіпотези допомагають виявити прогалини в аналітиці, сфокусувати подальший збір даних і дійти до точних узагальнень, висновків, прогнозів та оцінок.

Розробка та перевірка гіпотез набуває все більшого значення в рамках аналітичної розвідки. Гіпотези містять багато припущень і тому потребують перевірки (підтвердження, зміни або відхилення) аналітиками. Перевірка гіпотез повинна включати: аргументи «за» і «проти» гіпотези, її наслідки, огляд процесу мислення, а також збір і перегляд необхідних даних. Гіпотеза або будь-яке узагальнення мають містити відповіді на такі ключові запитання:

Хто? *Ключова особа/особи*

Що? *Кримінальна діяльність*

Як? *Використовувані методи*

Де? *Географічна інформація та сфера застосування*

Чому? *Мотив*

Коли? *Часовий проміжок*

Використання гіпотез для перевірки та дослідження кримінального явища або проблеми безпеки є важливим кроком у стратегічному мисленні,

> *переході від «скажи мені все, що ти знаєш» до конкретного діяльнісно-орієнтованого процесу.*
>
> *Цей технічний прийом та інші підкреслюють, що підготовка, рівень навичок і досвід як осіб, які приймають рішення, так і аналітиків є життєво важливими для успішного застосування ILP.*

Управління ООН з наркотиків і злочинності (UNODC) акцентує увагу на 9-ти ключових аналітичних методах, що забезпечують проактивний аналіз даних та інформації на усіх рівнях (стратегічному, оперативному та тактичному), а також обґрунтоване прийняття рішень й розвиток професійних знань [1; 15]. Зокрема:

> ***Аналіз патернів злочинності*** *є узагальненим виразом, що включає низку типів аналізу, зокрема виявлення тренду та аналіз «гарячих точок».*
>
> ***Аналіз демографічних/соціальних тенденцій*** *оцінює вплив соціально-економічних і демографічних змін на злочинність, а також демографічні зміни населення та безпритульність.*
>
> ***Аналіз мережі*** *оцінює напрям, частоту та силу зв'язків між спільниками злочинної мережі.*
>
> ***Профілі ринку*** *оцінюють певні кримінальні ринки, зокрема наркотиків або проституції тощо.*
>
> ***Профіль кримінального бізнесу*** *визначає бізнес-модель і методи, які використовують правопорушники або організовані злочинні групи.*
>
> ***Аналіз ризиків*** *оцінює масштаби ризиків або загроз, які є наслідком діяльності окремих злочинців або угруповань, для окремих потенційних жертв, поліції та громадськості.*
>
> ***Аналіз цільового профілю*** *описує злочинця, його сильні та слабкі сторони, спосіб життя, зв'язки, злочинну діяльність та потенційні точки перетину в житті цільового правопорушника.*
>
> ***Оцінка оперативної аналітики*** *визначає, чи відповідає збір інформації попередньо узгодженим цілям, а також виявляє прогалини в здійсненні оперативної аналітики (застосовується у масштабних проектах та операціях).*
>
> ***Аналіз результатів*** *оцінює ефективність правоохоронної діяльності та відстежує хід виконання планів.*

У додаток до вищезгаданого, крім методів аналізу, аналітики використовують низку інших методів якісного аналізу, що мають спільну мету: вони є інструментами для поділу складних проблем на більш керовані аналітичні частини.

ЗВІТУВАННЯ ТА ПОШИРЕННЯ АНАЛІТИЧНИХ ПРОДУКТІВ

Останнім кроком в аналітичному процесі є поширення аналітичного продукту та ознайомлення замовника (замовників) з його змістом.

Аналітичні продукти є результатом процесу аналітичної розвідки та, як правило, поширюються у формі чітко структурованих і лаконічних звітів. Розвідувальні аналітичні звіти спрямовані на відображення об'єктивної та точної інформації, а також виявлення та надання рекомендацій щодо ефективних стратегічних, оперативних чи тактичних рішень. Для забезпечення практичної цінності аналітичних продуктів, вони завжди мають бути чіткими та лаконічними. Як підкреслювалося раніше, тісна співпраця між аналітиком і замовником, включаючи організацію регулярних оглядових сесій, є невід'ємною складовою забезпечення цільового аналітичного продукту та представлення його результатів.

Замовниками розвідувального аналізу можуть бути слідчі, прокурори, керівництво правоохоронних органів та інші поліцейські чи державні установи. Коли це можливо і доцільно, аналітичний продукт має бути представлений громадськості.

Це може бути корисним для правоохоронних органів шляхом підвищення обізнаності громадськості щодо конкретних тем (у рамках запобігання злочинності), підвищення рівня прозорості, наочності та отримання цінної інформації від громадськості у відповідь на опубліковані звіти. Важливо вибрати правильний метод/формат для розповсюдження та представлення аналітичного продукту цільовій аудиторії та забезпечити його своєчасне надходження для підтримки рішень і дій.

Етап поширення є критично важливим для усієї архітектури ILP моделі, оскільки вона інформує замовника, а також усі належні підрозділи поліції щодо відповідної злочинної діяльності, явищ та злочинців. Через конфіденційність даних, які зазвичай подаються в аналітичних продуктах, необхідно прийняти чітке та зрозуміле правило, що базуватиметься на основних принципах «права знати» та «необхідності знати» відповідно до національних і міжнародних стандартів з прав людини та захисту даних.

Подальші відомості щодо поширення аналітичних продуктів мають бути викладені у відповідних національних довідниках чи посібниках відповідно до національних інструкцій і правових вимог, а також згідно з міжнародними стандартами з прав людини.

ЗВОРОТНИЙ ЗВ'ЯЗОК І ПОДАЛЬШІ ДІЇ

На цьому етапі аналітичного процесу ще раз необхідно підкреслити важливість активної співпраці між замовником та органом, який приймає рішення, а також аналітиком. Це також стосується оцінки аналітичного продукту та відгуків від замовника, який приймає рішення, або інших користувачів аналітичного продукту.

> *Аналітики та їхні менеджери повинні знати, чи відповідав продукт вимогам і чи сприяли рекомендації рішенням або подальшим діям.*

Аналітики також повинні отримувати відгуки про можливі покращення якості роботи. Корисною практикою є надсилання одержувачу форми зворотного зв'язку відразу після подання відповідного аналітичного звіту та інформаційних матеріалів.

Доречним є проведення організаційних заходів, зустрічей, нарад, під час яких обговорюватимуться аналітичні продукти, відгуки, співпраця та подальші рішення, дії чи операції. Такі заходи не тільки підвищують якість поставленого завдання, але також є необхідними для професійного розвитку.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *OSCE Guidebook Intelligence-Led Policing* (2017). TNTD/SPMU Publication. Series Vol. 13. Vienna. Retrieved from https://www.osce.org/files/f/documents/d/3/327476.pdf
2. Користін О.Є., Кирилюк О.С. Основи аналітичної розвідки в системі державної безпеки: навчальний посібник. Київ: Національна академія Служби безпеки України, 2023. 144 с.
3. Користін О.Є., Бабенко А.М., Заєць, К.Ю. Ісмайлов, В.А. Некрасов, Пефтієв Д.О. Основи кримінального аналізу: підручник; за заг. ред. Користіна О.Є., 2019. 296 с.
4. OSCE, Human rights in counter-terrorism investigations – A Practical Manual for Law Enforcement Officers (29 November 2013). Warsaw: Office for Democratic Institutions and Human Rights (ODIHR) and Transnational Threats Department (TNTD). Retrieved from www.osce.org/ odihr/108930?download=true
5. Practice Advice on Analysis (2008). National Policing Improvement Agency, Association of Chief Police Officers. Retrieved from library.college.police.uk/docs/npia/practice_advice_on_analysis_ interactive.pdf
6. UNODC. Criminal Intelligence – Manual for Managers (2011). Vienna: United Nations Publication. Retrieved from www.unodc.org/documents/organized-crime/Law-Enforcement/ Criminal_Intelligence_for_Managers.pdf

7. Oleksandr, Korystin & Nataliia, Svyrydiuk (22 March 2021). Activities of Illegal Weapons Criminal Component of Hybrid Threats. *Proceedings of the International Conference on Economics, Law and Education Research (ELER 2021),* 170, 86-91. DOI:10.2991/aebmr.k.210320.016
8. Nataliia, Svyrydiuk, Yaroslav, Likhovitskyy & Pavel Polián (27 August 2021). Information Threats in the Context of Hybrid War. Advances in Economics, Business and Management Research. *Proceedings of the International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research (BAMBEL 2021),* 188, 114-119. DOI:10.2991/aebmr.k.210826.020
9. EU Serious and Organised Crime Threat Assessment (SOCTA) 2021 (2021). Luxembourg: Publications Office of the European Union.
10. Korystin, Oleksandr & Svyrydiuk, Nataliia (2020). Methodological principles of risk assessment in law enforcement activity. *Nauka i Pravookhorona*, 3 (49), 191-198. DOI: 0.36486/np.2020.3(49)
11. Korystin, O.Y., Katamadze, G.S., Nekrasov, V.A., Mel'nyk, V.I. etc. (2021). *Fiscal Security of Ukraine – Threats, Risks, Vulnerabilities: Strategic vision*. Kherson: Vidavnichij Dim, Gelvetika, LLC.
12. Goldammer, P., Annen, H., Stöckli, P. L. & Jonas, K. (2020). Careless responding in questionnaire measures: Detection, impact, and remedies. *The Leadership Quarterly*, 31(4), 101384.
13. John, Rust, Michal, Kosinski & David, Stillwell (2021). *Modern psychometrics: the science of psychological assessment*. Milton Park, Abingdon, Oxon; New York. NY: Routledge.
14. Виноградов О.Г. Використання можливостей мови програмування та середовища R у психологічних дослідженнях: Т'юторіал з базових методів. *Український Психологічний Журнал*. 2020. Вип. 2(14). С. 28–63.
15. UNODC. Criminal Intelligence – Manual for Analysts (2011). Vienna: United Nations Publication. Retrieved from www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_ Intelligence_for_Analysts.pdf

DOI: https://doi.org/10.36486/978-966-2310-66-5-14

Хто володіє інформацією, той володіє світом.
У. Черчілль

РОЗДІЛ 14
Інформаційне забезпечення кримінального аналізу

Анатолій Мовчан
Юрій Крутік
Ганна Горбенко

Результативність діяльності правоохоронних органів безпосередньо залежить від якісного, своєчасного і достатнього інформаційно-аналітичного забезпечення. Відповідно до Положення про Департамент кримінального аналізу Національної поліції України, затвердженого наказом Національної поліції України від 29.12.2019 № 1354 [1], до основних завдань підрозділів кримінального аналізу належить, зокрема: організація та здійснення інформаційно-аналітичної діяльності для реалізації повноважень поліції; забезпечення формування та підтримка функціонування автоматизованих інформаційних систем, що утворюються в процесі здійснення оперативно-розшукової та аналітичної діяльності.

Основними *інформаційними ресурсами*, що використовуються в процесі інформаційно-аналітичного забезпечення підрозділів кримінального аналізу є:

- *оперативні обліки*, які складаються із оперативно-розшукових, оперативно-профілактичних та оперативно-довідкових обліків;
- *банки даних* кримінологічної, криміналістичної, адміністративної, статистичної інформації;
- *банки даних* інших міністерств, відомств, підприємств, установ та організацій, які не стосуються безпосередньо боротьби зі злочинністю;
- *банки даних* міських і обласних органів влади;
- *об'єкти* надання та отримання охоронних послуг;
- *оператори* мобільного зв'язку;
- *звернення та заяви* громадян, депутатські запити;
- *медіа*, у тому числі мережа Інтернет;
- *інформація*, отримана від суб'єктів, які здійснюють заходи у сфері протидії злочинності;
- *інформація*, отримана від правоохоронних органів іноземних держав та міжнародних правоохоронних організацій;
- *інформація*, отримана від громадських (неурядових) організацій, у тому числі міжнародних.

Єдина інформаційна система МВС (ЄІС МВС) призначена для автоматизації та технологічного забезпечення обміну даними між суб'єктами єдиної інформаційної системи МВС, зокрема в інтересах національної безпеки, захисту прав та законних інтересів громадян, суспільства і держави [2].

Функціональними підсистемами ЄІС МВС є:

- Національна система біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства;
- Інформаційний портал Національної поліції України;
- Єдиний державний реєстр транспортних засобів;
- Реєстр адміністративних правопорушень у сфері безпеки дорожнього руху;
- Система фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі;
- Інтегрована міжвідомча інформаційно-комунікаційна система щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон;
- Інформаційно-комунікаційна система прикордонного контролю «Гарт-1»;
- Інформаційно-комунікаційна система 112;
- Електронний реєстр геномної інформації людини;
- Єдиний реєстр осіб, зниклих безвісти за особливих обставин;
- Єдиний реєстр зброї;
- Система управління силами та засобами цивільного захисту;
- інші системи, реєстри та бази (банки) даних, створені суб'єктами єдиної інформаційної системи МВС в межах реалізації владних повноважень.

У ході здійснення інформаційно-аналітичної діяльності підрозділи кримінального аналізу використовують інформацію, яка обробляється та зберігається в автоматизованих інформаційних системах МВС України та Національної поліції України.

Зокрема, у Національній поліції створена і функціонує ***Інформаційно-комунікаційна система «Інформаційний портал Національної поліції України» (ІКС ІПНП)*** – як сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються в процесі діяльності Національної поліції та її інформаційно-аналітичного забезпечення.

ДІАП Національної поліції забезпечує наповнення та підтримку в актуальному стані баз (банків) даних, що входять до ЄІС МВС через ІКС ІПНП, стосовно:

1) *осіб*, щодо яких поліцейські здійснюють профілактичну роботу;
2) *виявлених* кримінальних та адміністративних правопорушень, осіб, які їх учинили, руху кримінальних проваджень;
3) *обвинувачених*, обвинувальний акт щодо яких надіслано до суду;
4) *розшуку* підозрюваних, обвинувачених (підсудних) осіб, які ухиляються від відбування покарання або вироку суду;
5) *розшуку* безвісно відсутніх осіб;
6) *установлення* особи невпізнаних трупів та людей, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком;
7) *зареєстрованих* в установленому порядку кримінальних або адміністративних правопорушень, подій, які загрожують особистій чи публічній безпеці, надзвичайних ситуацій;
8) *осіб*, затриманих за підозрою у вчиненні правопорушень (адміністративне затримання, затримання згідно з дорученнями уповноважених органів, затримання осіб органами досудового розслідування, адміністративний арешт, домашній арешт);
9) *осіб*, які скоїли адміністративні правопорушення, провадження у справах за якими здійснюється поліцією;
10) *зареєстрованих* кримінальних та адміністративних корупційних правопорушень, осіб, які їх учинили, та результатів розгляду цих правопорушень у судах;
11) *іноземців* та осіб без громадянства, затриманих поліцією за порушення визначених правил перебування в Україні;
12) *викрадених* номерних речей, цінностей та іншого майна, які мають характерні ознаки для ідентифікації, або речей, пов'язаних з учиненням правопорушень, відповідно до заяв громадян;
13) *викрадених* (втрачених) документів за зверненням громадян;
14) *знайдених, вилучених* предметів і речей, у тому числі заборонених або обмежених в обігу, а також документів з ознаками підробки, які мають індивідуальні (заводські) номери;
15) *транспортних* засобів, які розшукуються, у тому числі у зв'язку з безвісним зникненням особи, виявлених безгосподарних транспортних засобів, а також викрадених, втрачених номерних знаків;
16) *зброї*, що перебуває у володінні та користуванні фізичних і юридичних осіб, яким надано дозвіл на придбання, зберігання, носіння, перевезення зброї;
17) *відомостей*, що накопичуються в процесі здійснення ОРД в частині, що стосується розшуку осіб які переховуються від органів влади, безвісно зниклих, встановлення особи громадян за невпізнаними трупами та осіб, які не здатні через стан здоров'я, вік або інші причини повідомити інформацію про себе;
18) *інших* власних баз даних, необхідних для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчих інформаційно-аналітичних систем, необхідних для виконання покладених ДІАП повноважень[3; 4].

Автоматизована інформаційна система оперативного призначення ЄІС МВС (АІС ОП) є сукупністю програмно-технічних і комунікаційних засобів та призначена для накопичення й обробки відомостей, що утворюються в процесі оперативно-розшукової діяльності Національної поліції України.

Основними завданнями АІС ОП є:

- підвищення рівня інформаційно-аналітичного забезпечення ОРД Національної поліції;
- забезпечення процесу підтримки управлінських рішень керівництвом Національної поліції;
- об'єднання отриманої в процесі ОРД Національної поліції інформації в єдиному інформаційному просторі з використанням сучасних інформаційних технологій, комп'ютерного і комунікаційного обладнання;
- протидія злочинності та проведення профілактичної роботи, спрямованої на запобігання вчиненню правопорушень.

Функції АІС ОП:

1) автоматизація процесів обліку отриманої в процесі ОРД Національної поліції інформації;
2) збір, зберігання, пошук та узагальнення інформації;
3) відображення повнотекстової, графічної, табличної та статистичної інформації, а також фото- і відеозображень;
4) утворення електронного досьє;
5) формалізація технологічних процесів обробки інформації, визначення типових маршрутних технологічних схем для їх виконання;
6) забезпечення надійного зберігання інформаційних обліків та їх систематизація;
7) забезпечення комплексного захисту інформації та розмежування доступу до інформації, що зберігається в АІС ОП.

Інформаційними ресурсами АІС ОП є об'єктивно поєднаний набір відомостей, що безпосередньо стосуються осіб та подій (кримінальних правопорушень), які накопичуються в процесі здійснення ОРД Національної поліції. Розпорядником АІС ОП є Департамент кримінального аналізу Національної поліції України [5].

Поряд з обліками спеціального призначення (АІС ОП), які формують і використовують оперативні підрозділи Національної поліції, створені обліки загального користування, які ведуть слідчі, криміналістичні підрозділи, сервісні центри, поліція охорони тощо. Крім оперативних обліків, відповідно до напряму функціонування галузевих служб Національної поліції, розрізняють кримінологічні, криміналістичні, адміністративні обліки.

Інформаційно-аналітична система «Облік відомостей про притягнення особи до кримінальної відповідальності та наявності судимості» (ІАС) – це структурована автоматизована база даних, яка використовується для збирання, зберігання, обліку, пошуку, узагальнення, захисту, перевірки достовірності відомостей, перетворення та відображення інформації, забезпечення доступу до даних про притягнення особи до кримінальної відповідальності, відсутність (наявність) судимості або обмежень, передбачених кримінальним процесуальним законодавством України.

Об'єктами обліку ІАС є:
- фізичні особи, які відповідно до КПК України набули статусу підозрюваного, обвинуваченого (підсудного), засудженого;
- фізичні особи, щодо яких застосовано примусові заходи медичного чи виховного характеру;
- фізичні особи, яких звільнено від кримінальної відповідальності згідно із статтями 44-49, 97 Кримінального кодексу України;
- фізичні особи, яких оголошено в розшук;
- громадяни України, яких засуджено судами інших держав;
- архівна інформація репресивних органів.

Джерелами автоматичного наповнення ІАС є такі інформаційні системи:
- Єдиний реєстр досудових розслідувань щодо осіб, яким повідомлено про підозру; осіб, щодо яких обрано запобіжний захід; наслідків досудового розслідування кримінальних правопорушень;
- Єдиний державний реєстр судових рішень щодо наслідків судового розгляду кримінальних проваджень;
- Єдиний реєстр засуджених та осіб, узятих під варту, щодо засуджених, ув'язнених та суб'єктів пробації;
- оцифровані архівні інформаційні масиви персонально-довідкового обліку МВС [6].

Єдиний державний реєстр транспортних засобів (ЄДРТЗ) – це інформаційна система, яка є функціональною підсистемою ЄІС МВС, що забезпечує накопичення, використання, узагальнення, зберігання, передачу, захист інформації про зареєстровані транспортні засоби, їх власників (співвласників), належних користувачів, закріплені номерні знаки та реєстраційні документи на такі транспортні засоби.

Основними інформаційними об'єктами ЄДРТЗ є набір відомостей про:
- зареєстровані на території України транспортні засоби та їх власників (співвласників), належних користувачів;
- закріплені номерні знаки та реєстраційні документи на такі транспортні засоби.

Пошук відомостей в ЄДРТЗ здійснюється за одним з таких критеріїв:
- прізвище, ім'я, по батькові (за наявності) власника (належного користувача) та дата його народження;
- реєстраційний номер облікової картки платника податків або серія (за наявності) та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків відповідно до законодавства);
- повне найменування юридичної особи;

- ідентифікаційний код юридичної особи в Єдиному державному реєстрі підприємств та організацій України;
- дата або період, за який здійснюється пошук;
- номерний знак запитуваного транспортного засобу;
- інші критерії, відповідно до законодавства [7].

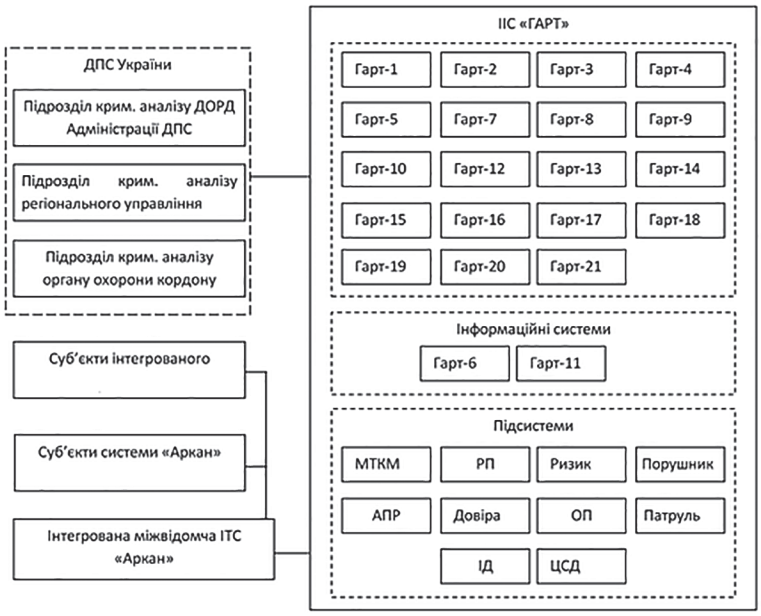
Система дозволяє експортувати отримані в результаті пошуку дані у інформаційну таблицю формату Microsoft Excel, в якій відображаються всі реєстраційні дані про транспортний засіб, про власника та про уповноважену особу.

Інформаційна підсистема «Гарпун» ІКТ «Інформаційний портал Національної поліції України». ІП «Гарпун» призначена для обробки відомостей про транспортні засоби усіх типів (автомобілі, автобуси, мотоцикли всіх типів, марок і моделей, самохідні машини, причепи та напівпричепи до них, мотоколяски, інші прирівняні до них ТЗ та мопеди) та номерні знаки ТЗ, що розшукуються у рамках кримінального, виконавчого проваджень, проваджень у справах про адміністративні правопорушення, оперативно-розшукової діяльності, а також за ухвалою слідчого судді, суду.

Обліку в ІП «Гарпун» за категоріями «орієнтування про незаконне заволодіння ТЗ», «орієнтування про залишення ТЗ місця дорожньо-транспортної пригоди», «орієнтування про залишення ТЗ місця вчинення іншого правопорушення» та «орієнтування оперативне про ТЗ» підлягають відомості про розшук ТЗ, які стали засобом, предметом кримінального чи адміністративного правопорушення або місцезнаходження яких встановлюється під час здійснення оперативно-розшукової діяльності.

Для аналітичної обробки використовується фото- і відеоінформація, отримана з технічних засобів та технічних приладів, які мають функції фото- і відеофіксації (запису), закріплених поліцією на службових ТЗ, монтованих/розміщених по зовнішньому периметру доріг і будівель, а також інформація, отримана з автоматичної фото- і відеотехніки, що знаходиться в чужому володінні [8].

У діяльності підрозділів кримінального аналізу використовується електронні інформаційні ресурси прикордонного відомства, що зосереджено в ***інтегрованій інформаційній системі прикордонного відомства «Гарт».***



Така система являє собою комплекс взаємопов'язаних інформаційних систем, підсистем, засобів комунікації, які функціонують у єдиному інформаційному просторі прикордонного відомства, регламентуються відповідними організаційними та розпорядчими керівними документами та призначені для інформаційного супроводу посадових осіб Державної прикордонної служби України.

Інтегрована інформаційна система «Гарт» призначена для автоматизації завдань та процесів суб'єктів системи щодо виконання ними завдань із оперативно-розшукової, оперативно-службової та інформаційно-аналітичної діяльності органів та підрозділів Державної прикордонної служби України.

Основою інтегрованої інформаційної системи є комунікаційна мережа ДПС України, на якій розгорнуті інформаційно-комунікаційні системи, інформаційна система, АРМ та різні програмно-технічні комплекси.

Особливістю комунікаційної мережі Державної прикордонної служби України є те, що вона суто відомча та не має виходу до всесвітньої глобальної мережі Інтернет, функціонування інформаційних складових здійснюється з використанням орендованих каналів зв'язку, забезпечує обмін критичною інформацією щодо прийняття рішень між суб'єктами інтегрованого управління кордонами.

Однією із основних інформаційних систем, що використовується підрозділами кримінального аналізу для отримання даних в рамках аналітичних досліджень є ***«Гарт-1».***

Система «Гарт-1» створюється і використовується в інтересах розвідки, контррозвідувального забезпечення охорони державного кордону України, оперативно-розшукової діяльності, участі в боротьбі з організованою злочинністю та протидії незаконній міграції з метою своєчасного та достовірного інформаційно-аналітичного забезпечення діяльності підрозділів та органів Державної

прикордонної служби України для здійснення ними заходів із запобігання і недопущення в'їзду в Україну або виїзду з України осіб, яким згідно із законодавством не дозволяється в'їзд в Україну або тимчасово обмежено право виїзду з України, у тому числі згідно з дорученнями правоохоронних органів, розшуку в пунктах пропуску через державний кордон осіб, які переховуються від органів дізнання, слідства та суду, ухиляються від відбуття кримінальних покарань, посилення контролю за додержанням правил в'їзду, виїзду, перебування в Україні іноземців та осіб без громадянства, а також виконання інших завдань у правоохоронній сфері згідно із законодавством.

Функціями системи «Гарт-1» є:

- *формування баз даних про осіб, які перетнули державний кордон Україні, у тому числі з фіксуванням їх біометричних даних, осіб, яким згідно із законодавством не дозволяється в'їзд в Україну або тимчасово обмежено право виїзду з України, у тому числі згідно з дорученнями правоохоронних органів, осіб, які переховуються від органів дізнання, слідства та суду, ухиляються від відбуття кримінальних покарань, недійсних, викрадених і втрачених документів на право виїзду за кордон та інших баз даних, що створюються та використовуються відповідно до законодавства;*
- *автоматизація процесів перевірки відомостей про осіб, які перетинають державний кордон України, за базами даних осіб, яким згідно із законодавством не дозволяється в'їзд в Україну або тимчасово обмежено право виїзду з України, у тому числі згідно з дорученнями правоохоронних органів, осіб, які переховуються від органів дізнання, слідства та суду, ухиляються від відбуття кримінальних покарань, недійсних, викрадених і втрачених документів на право виїзду за кордон та іншими базами даних, що створюються та використовуються відповідно до законодавства;*
- *надання користувачам доступу до інформації, що зберігається в системі «Гарт-1»;*
- *забезпечення комплексного захисту інформації та розмежування доступу до інформації, що зберігається в базах даних системи «Гарт-1».*

Для роботи з інформацією, що отримана з автоматизованої інформаційно-аналітичної системи та інформаційні ресурси аналітики використовують ***базу даних «iBase»***, що інтегрована в «Гарт-10».

База даних «iBase» – дозволяє збирати і аналізувати дані з різних джерел в повністю контрольованому середовищі. «iBase» спеціально спроектований для кримінальних аналітиків і має потужний функціонал, націлений на аналіз.

«iBase» розрахований на значну кількість користувачів і є системою, що дозволяє одночасно працювати команді кримінальних аналітиків. Крім того, «iBase» надає можливість одночасної роботи з багатьма базами даних типу Access, SQL Server й інших та створювати копію робочої бази даних, щоб працювати автономно і автоматично вносити будь-які зміни в загальну базу даних.

«iBase» використовується щодо супроводу оперативно-розшукових заходів спрямованих на:

- *боротьбу з тероризмом;*
- *боротьбу із організованою злочинністю;*
- *боротьбу зі злочинами в сфері високих технологій;*
- *розкриття тяжких та особливо тяжких злочинів;*
- *боротьбу з незаконним обігом зброї та наркотиків;*
- *боротьбу зі злочинами в сфері автомобільного бізнесу;*
- *пошук осіб зниклих без вести;*
- *боротьбу з виробництвом і розповсюдженням контрафактної продукції;*
- *організацію безпеки масових заходів;*
- *забезпечення безпеки діяльності правоохоронних органів;*
- *проведення аналітичної розвідка.*

База даних «iBase» функціонально поєднана зі спеціальним програмним забезпеченням «Analyst's Notebook», що дозволяє:

поглиблено й ефективно проводити аналіз системи взаємопов'язаних об'єктів і динаміки послідовних подій. При цьому результати дослідження відображаються у вигляді зручних для розуміння схем і діаграм;

*створювати схеми за допомогою запитів до реляційних баз даних, а також імпорту даних з *. Txt і *. Xml файлів. За допомогою наявних функцій можна об'єднувати елементи діаграм, шукати існуючі між ними зв'язки, використовувати систему пошуку елементів, простежувати «шлях», який об'єднує об'єкти, тощо;*

швидко виявити суть проблеми і визначити правильний напрямок подальшої роботи, чому сприяє широкий вибір інструментів для розташування, копіювання, оновлення і пошуку зображених на діаграмі об'єктів, об'єднання діаграм і їх масштабування;

у графічній формі сформулювати запит для пошуку об'єктів та виявлення їх зв'язків, а також створювати шаблони подій. Піктограми у «Analyst's Notebook» є не тільки символічним

представленням інформації, вони безпосередньо пов'язані із записами в базі даних, що дозволяє переглянути або відредагувати вихідну інформацію.

Розглянуті вище внутрішні масиви інформації, накопичені підрозділами кримінального аналізу в ході здійснення оперативно-службової діяльності є самодостатніми та самостійними, але їх спільне використання дозволяє максимально ефективно здійснювати пошук інформації з мінімальною затратою часу.

Взаємодія з органами виконавчої влади здійснюється ***ІПС «Гарт» через інформаційно-телекомунікаційну систему «Аркан»***, яка надає можливість здійснювати обмін даними при перетині державного кордону особами, транспортними засобами, вантажами.

Система «Аркан» створена з метою своєчасного, достовірного та функціонально повного інформаційно-аналітичного забезпечення діяльності суб'єктів системи стосовно здійснення ними заходів із запобігання і недопущення в'їзду в Україну або виїзду з України осіб, яким згідно із законодавством не дозволяється в'їзд в Україну або яких тимчасово обмежено в праві виїзду з України, у тому числі згідно з дорученнями правоохоронних органів, розшуку в пунктах пропуску через державний кордон осіб, які переховуються від органів дізнання, слідства та суду, ухиляються від відбуття кримінальних покарань, припинення протиправної діяльності фізичних і юридичних осіб, які незаконно переправляють мігрантів в Україну або транзитом переміщують їх через територію України, посилення контролю за додержанням правил в'їзду, виїзду, перебування в Україні іноземців та осіб без громадянства, а також виконання інших завдань у правоохоронній сфері згідно із законодавством [9].

Функції системи «Аркан»:

- поповнення інформаційних ресурсів (баз даних) інформаційних систем органів виконавчої влади у режимі обробки повідомлень;
- надання суб'єктам системи «Аркан» інформації з інформаційних ресурсів (баз даних) інформаційних систем органів виконавчої влади;
- забезпечення двосторонніх інформаційно-телекомунікаційних зв'язків між суб'єктами системи «Аркан»;
- здійснення електронного документообігу між суб'єктами системи «Аркан»;
- забезпечення комплексного захисту інформації та розмежування доступу до інформаційних ресурсів (баз даних) суб'єктів системи «Аркан».

У системі «Аркан» обробляється інформація, яка є власністю держави і створюється в процесі поточної діяльності органів виконавчої влади - суб'єктів системи «Аркан». Ця інформація підлягає захисту. За режимом доступу інформація, яка обробляється в системі «Аркан», поділяється на відкриту інформацію та інформацію з обмеженим доступом. Інформація з обмеженим доступом за правовим режимом є конфіденційною інформацією, якій надається гриф обмеження доступу «Для службового користування».

Інформація в системі «Аркан» повинна оброблятися із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Її завданням є забезпечення унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації, що обробляється в системі «Аркан». Достовірність інформації, яка обробляється в системі «Аркан», забезпечується застосуванням електронного цифрового підпису в порядку, визначеному Законами України «Про електронний цифровий підпис» і «Про електронні документи та електронний документообіг».

Бази даних, які входять в систему «Аркан» містять відомості:

- про осіб, яким СБУ заборонено в'їзд в Україну, відомості про осіб, стосовно яких є доручення СБУ;
- про транспортні засоби, стосовно яких є доручення СБУ;
- про осіб, стосовно яких є доручення СЗРУ;
- про осіб, яким МВС заборонено в'їзд в Україну;
- про осіб, стосовно яких є доручення МВС;
- про втрачені, викрадені та оголошені недійсними документи, що дають право на виїзд з України та в'їзд в Україну;
- про транспортні засоби, що перебувають у розшуку;
- про фізичних осіб, які перебувають у розшуку;
- про транспортні засоби, зареєстровані в Україні, у тому числі на підставі виданих митними органами посвідчень на право реєстрації та вантажних митних декларацій;
- про викрадені предмети культурної спадщини;
- про транспортні засоби, стосовно яких є доручення МВС;
- про осіб, яким органами охорони державного кордону заборонено в'їзд в Україну;
- про осіб, стосовно яких виконано доручення правоохоронних органів, у тому числі СБУ і МВС;

- про вилучені, утрачені, викрадені та оголошені недійсними документи, що дають право на виїзд/в'їзд в Україну;
- про затримані транспортні засоби, які перебувають у розшуку;
- відомості про документи, видані установами МЗС і МВС, у яких виявлено несправності під час здійснення паспортного контролю;
- про візи, видані установами МЗС, у яких виявлено несправності під час здійснення паспортного контролю;
- про осіб, які перетнули державний кордон;
- відомості про осіб, яким органами охорони державного кордону відмовлено у перетинанні державного кордону;
- про осіб, яких затримано за організацію незаконного переміщення через державний кордон;
- про іноземців та осіб без громадянства, які не виїхали з України по закінченні строку перебування в Україні;
- відомості про транспортні засоби, стосовно яких виконано доручення СБУ і МВС;
- про втрачені, викрадені та оголошені недійсними документи громадян України для виїзду за кордон, видані МЗС, дипломатичними представництвами та консульськими установами України за кордоном;
- про документи, що дають право на в'їзд та виїзд з України, оформлені МЗС та дипломатичними представництвами і консульськими установами України за кордоном;
- про іноземців та осіб без громадянства, яким оформлено візи для в'їзду в Україну;
- про іноземців та осіб без громадянства, яким оформлено дозволи на перебування в Україні;
- про митне оформлення транспортних засобів, які перетинають митний кордон;
- про перетинання вантажами митного кордону;
- про порушників митного законодавства;
- про юридичних та фізичних осіб - підприємців, які перебувають на податковому обліку (з метою перевірки правових підстав в'їзду і реєстрації іноземців та осіб без громадянства); про осіб, стосовно яких є доручення ДПА.

Оперативні підрозділи Державної прикордонної служби України використовують інформацію отриману з системи «Аркан» при здійсненні кримінального аналізу. Зокрема, використовується інформація стосовно осіб, які перетинають або перетинали державний кордон України. Така інформація дозволяє встановити безпосередньо факт перетину державного кордону (напрям, дату, час, транспортний засіб а дані осіб, які прямують разом) особою, відносно якої перевіряється інформація, а також встановити з числа подорожуючих коло осіб, з якими дана особа має ділові або родинні зв'язки.

Система «Аркан» дозволяє експортувати отримані в результаті пошуку дані у таблиці формату Microsoft Excel для подальшої обробки. Експорт здійснюється за стандартними шаблонами наповненість яких достатня для аналітичної роботи.

Єдина інформаційно-аналітична система управління міграційними процесами (ЄІАС УМП) включає в себе підсистеми «Адміністративні правопорушення» і «Облік іноземців та біженців». Засобами підсистеми «Адміністративні правопорушення» оформляються усі справи про адмінправопорушення, розгляд яких віднесено до компетенції ДМС, у тому числі – за протоколами, складеними працівниками Державної прикордонної служби України та інших органів.

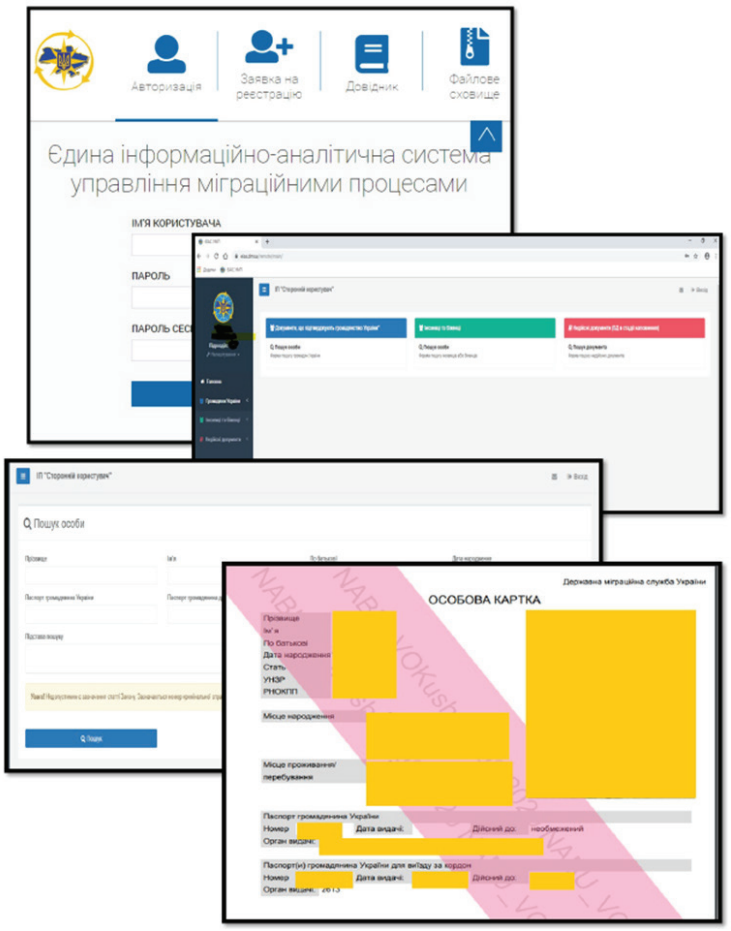
Державна міграційна служба України забезпечує надання інформації щодо:

- *реєстрації* місця проживання або місця перебування особи;
- *документів*, що посвідчують особу, підтверджують громадянство України або спеціальний статус особи;
- *імміграції* в Україну;
- *осіб*, які отримали або претендували на отримання статусу біженця чи особи, яка потребує додаткового захисту, осіб, які набули (припинили) громадянство України, та осіб, яким надано (скасовано) дозвіл на імміграцію в Україну.

ІС «ДМС» використовується для отримання інформації про персональні данні щодо громадян України (фото, ПІБ, дата народження, УНЗР, РНОКПП, стать, місце народження, номер телефону, адреса реєстрації /проживання, документи: паспорт громадянина України, закордонний паспорт, свідоцтво про народження), іноземців та біженців (фото, ПІБ на українській та латиниці, дата народження, категорія обліку, громадянство, документи, тощо), а також інформацію про недійсні документи.

З допомогою інформаційної підсистеми ЄІАС УМП «Облік іноземців та біженців» здійснюється ефективний контроль за видачею документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус – для запобігання їх підробленню або незаконному використанню. Також у підсистемі, з метою оперативної перевірки поданих іноземцями та особами без громадянства документів, налагоджено інформаційну взаємодію з МЗС щодо перевірки виданих віз [10].

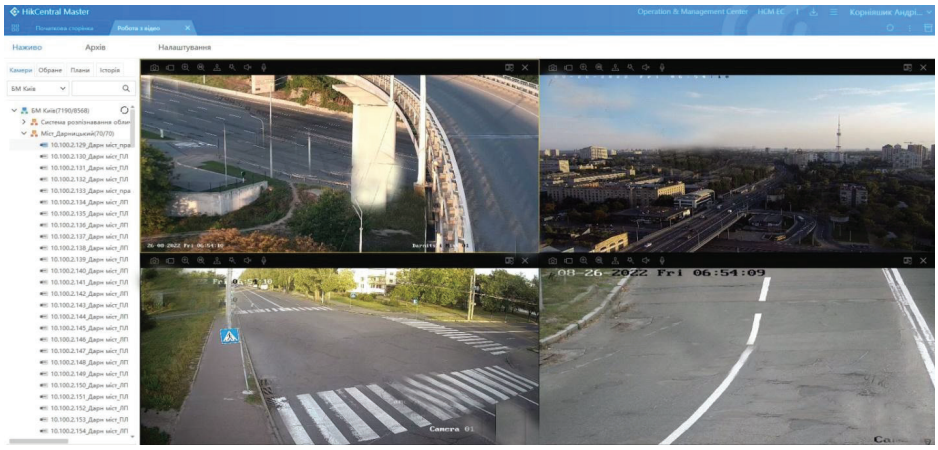
Організація доступу до інформаційних ресурсів МВС, ДМС та Держприкордонслужби визначається Порядком організації доступу до інформаційних ресурсів під час інформаційної взаємодії між Міністерством внутрішніх справ України, Державною міграційною службою України та Державною прикордонною службою України [11].



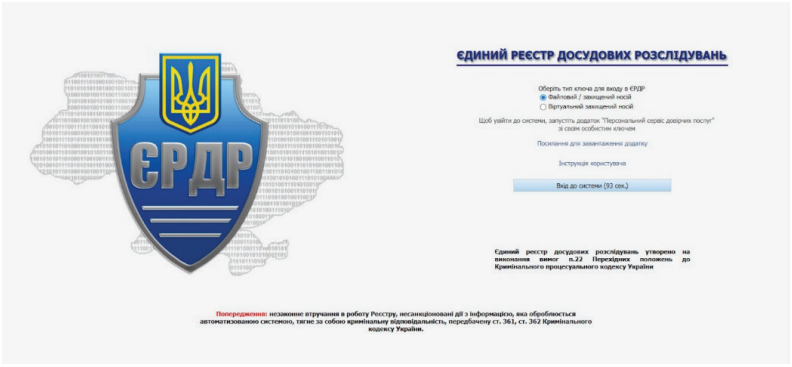
Система відеоспостереження «Безпечне місто» створена та використовується для посилення безпеки населення, дорожнього руху і розкриття злочинів. Усі відеокамери пов'язані між собою в єдину систему, яка записує та аналізує інформацію.

Унікальний модуль дозволяє шукати правопорушників не лише завдяки спеціалізованим камерам розпізнавання обличчя. Модуль фіксує зображення з будь-якої камери, що встановлена в рамках мережі та порівнює їх із базою правопорушників, що була створена правоохоронними органами. Якщо система виявляє подібність, оператор одразу отримує тривожний сигнал. Таким чином, система прискорює розшук злочинців та правопорушників [12].

Зараз камери розташовані у місцях великого скупчення людей: у дошкільних навчальних закладах, школах, метрополітені, вокзалах, лікарнях тощо. Система також дозволяє переглядати відео із підключених камер як у режимі реального часу, так і архівні записи. Також наявна можливість пошуку автомобіля за номерними знаками, перегляд його маршрутів руху, встановлення транспортних засобів, що їздять поруч та постановка конкретних т/з на контроль.



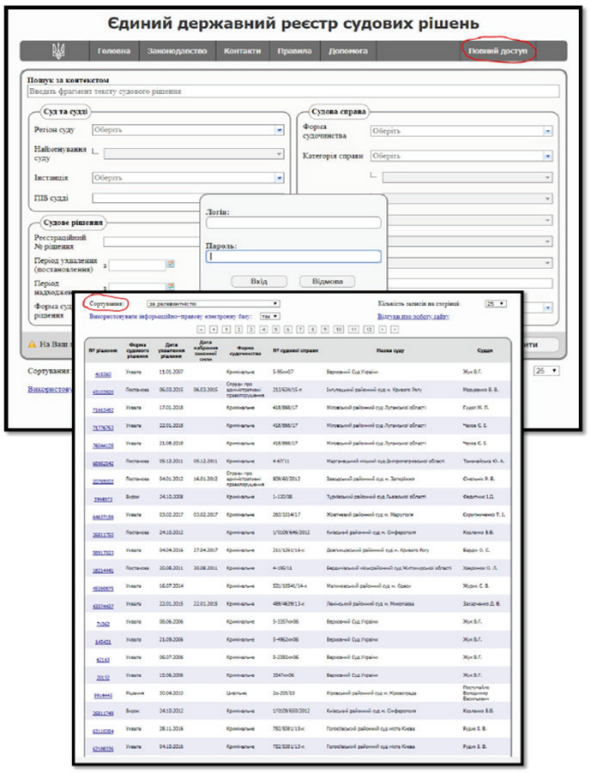
Єдиний реєстр досудових розслідувань – це електронна інформаційно-комунікаційна система, призначена для збирання, зберігання, захисту, оброблення, обліку, пошуку, узагальнення даних, які використовуються для формування звітності, а також надання інформації про відомості, внесені до Реєстру, з дотриманням вимог кримінального процесуального законодавства та законодавства, яким урегульовано питання захисту персональних даних та доступу до інформації з обмеженим доступом.



Суб'єкти інформаційних відносин відповідно до своїх повноважень, визначених законодавством, спільно встановлюють перелік відомостей, структуру та формат інформаційних файлів, що передаються та приймаються в порядку інформаційної взаємодії, процедури взаємодії інформаційних систем, форми журналів обліку інформаційних файлів обміну, а також визначають відповідальні структурні підрозділи суб'єктів інформаційних відносин, державні підприємства, установи, які

належать до сфери управління суб'єктів інформаційних відносин, що забезпечують та здійснюють організаційне та технічне супроводження автоматизованого обміну інформацією, та відповідно до цього Порядку та своїх повноважень приймають спільні рішення, які оформлюють окремими протоколами [13].

Єдиний державний реєстр судових рішень - державна інформаційна система, що входить до складу Єдиної судової інформаційної системи і забезпечує збирання, облік (реєстрацію), накопичення, зберігання, захист, пошук та перегляд інформаційних ресурсів Реєстру та їх образів.



Доступ до Реєстру здійснюється через веб-інтерфейс та складається з розділів:

Головна. Містить поля вводу параметрів для виконання пошуку документів. Пошук виконується за текстом судового рішення або за розширеними параметрами. Результати пошуку відображаються у вигляді таблиці з посиланнями на документ.

Законодавство. Містить посилання на законодавчі документи. Для того, щоб переглянути документ, необхідно натиснути на посилання. У новому вікні відобразиться текст документа.

Контакти. Містить інформацію про реквізити інформаційно-технічного адміністратора ЄДРСР: найменування, адреса, номер телефону та інтерфейс для відправлення повідомлення.

Правила. Містить інформацію про правила роботи з Єдиним державним реєстром судових рішень.

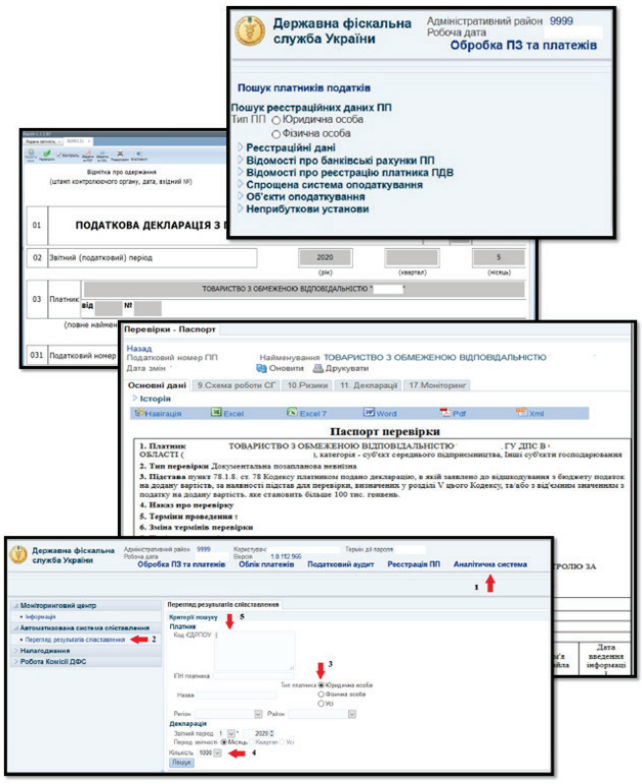
Допомога. Містить інформацію про користування сайтом, його можливості та зміст.

Повний доступ. Виводить додаткову форму для реєстрації фахівців, що відповідно до законодавства мають право на повний доступ до даних Реєстру.

З дня початку функціонування Єдиної судової інформаційно-телекомунікаційної системи Реєстр переходить до її складу [14]. Повний доступ до інформаційних ресурсів Реєстру забезпечується за допомогою електронного кабінету виключно для авторизованих користувачів.

Інформаційна система «Податковий блок»

ІС «Податковий блок» використовується для отримання інформації про податковий облік (податкова та фінансова звітність, ІР, сплачені податки, податковий борг, податкові перевірки) та реєстраційні дані платників податків (засновник/керівник/бухгалтер, розмір статутного капіталу, адреса, банківські рахунки, рахунки в цінних паперах, відокремленні підрозділи, тощо).



Підсистема «Обробка податкової звітності та платежів». Наведена підсистема надає можливість здійснювати перегляд поданої до ДПС податкової звітності зі всіма додатками в режимі online. Підсистема дозволяє проводити пошук податкової звітності, як по окремій декларації, так і по вибраному платнику податків.

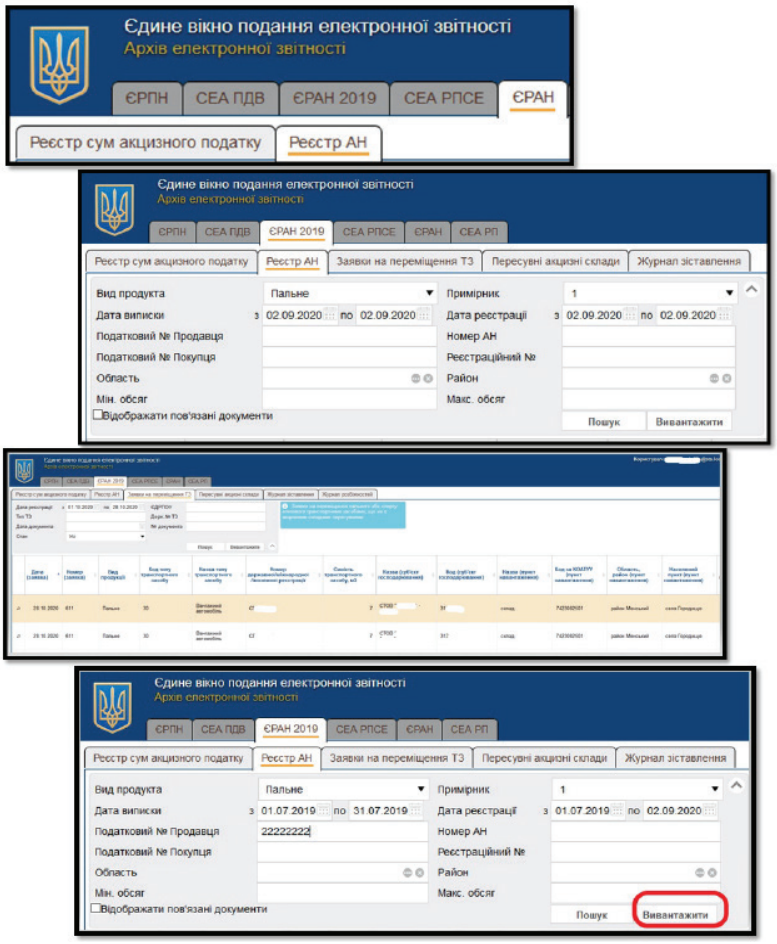
Підсистема «Облік платежів» містить інформацію про стан розрахунків платників податків з бюджетом та надає можливість переглядати інформацію по картці особового рахунку вибраного платника податку щодо наявності переплати, недоїмки, пені та інших операцій в розрізі кожного податку.

Підсистема «Податковий аудит» дозволяє перевіряти інформацію щодо проведених планових, позапланових документальних та камеральних перевірок платників податку. Підсистема надає можливості встановлення інформації щодо підстав проведення перевірки, періоду охопленого перевіркою та її результатів.

Підсистема «Реєстрація платників податків» акумулює інформацію щодо реєстраційних даних суб'єктів господарювання та змін до них отриманими ДПС від уповноваженого органу з питань державної реєстрації, на який покладено функцію ведення Єдиного державного реєстру. Підсистема в тому числі містить інформацію щодо адрес реєстрації, посадових осіб, засновників, банківських рахунків, податкову звітність платників податків.

Аналітична система надає можливість в автоматизованому режимі переглядати результати співставлення податкових зобов'язань та податкового кредиту з ПДВ в розрізі контрагентів.

Єдиний реєстр акцизних накладних



Система електронного адміністрування реалізації пального та спирту етилового. Дана система стосується всіх суб'єктів господарювання, що здійснюють реалізацію пального, спирту етилового, включаючи всі стадії обігу пального на митній території України – від їх виробника/імпортера до суб'єктів господарювання, які реалізують пальне та етиловий спирт кінцевому споживачу.

Єдиний реєстр акцизних накладних складається з наступних підсистем:

- *реєстр сум акцизного податку;*
- *реєстр АН;*
- *заявки на переміщення ТЗ;*
- *пересувні акцизні склади;*
- *журнал зіставлення/ журнал розбіжностей.*

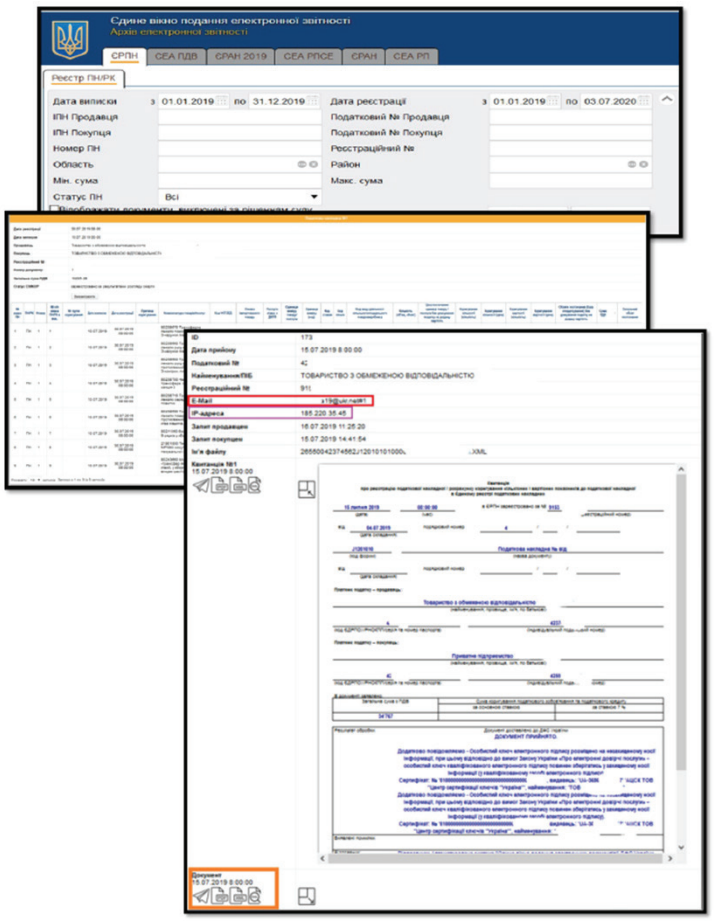
Підсистема «Реєстр АН» надає можливість здійснювати перегляд акцизних накладних/розрахунків коригування та квитанцій в реальному часі.

Підсистема «Заявки на переміщення ТЗ» надає можливість здійснювати перегляд заявок суб'єктів господарювання, які не є розпорядниками акцизних складів та здійснюють переміщення на митній території України власного пального або спирту етилового для потреб власного споживання чи промислової переробки.

Підсистема «Пересувні акцизні склади» надає можливість здійснювати перегляд інформації про пересувні акцизні склади – транспортні засоби (автомобільний, залізничний, морський, річковий, повітряний, магістральний трубопровід), на яких переміщується та/або зберігається пальне або спирт етиловий на митній території України.

Підсистема «Журнал зіставлення/Журнал розбіжностей» надає можливість здійснювати перегляд результатів співставлення показників Системи електронного адміністрування реалізації пального та спирту етилового та Єдиного державного реєстру витратомірів-лічильників та рівнемірів-лічильників рівня пального/ Єдиного державного реєстру витратомірів-лічильників обсягу виробленого спирту етилового понад встановлені допустимі значення.

Підсистема «Реєстр сум акцизного податку» надає можливість здійснювати перегляд зареєстрованих заявок на поповнення/коригування обсягу залишку пального/спирту (зобов'язання по акцизу) та отримувати інформацію про поповнення акцизного рахунку.



Єдиний реєстр податкових накладних (ЄРПН) використовується для отримання інформації про видані та отримані податкові накладні (розрахунки коригування до податкових накладних) за запитуваний період по визначеній юридичній особі або фізичній особі-підприємцю, які зареєстровані платниками податку на додану вартість.

В ЄРПН містяться такі типи документів:

- *податкова накладна - електронний документ, який складається платником податку на додану вартість відповідно до вимог податкового кодексу України в електронній формі у затвердженому в установленому порядку форматі (стандарті) та надсилається для реєстрації;*
- *розрахунок коригування електронний документ, який складається платником податку на додану вартість відповідно до вимог податкового кодексу України в електронній формі у затвердженому в установленому порядку форматі (стандарті) та надсилається для реєстрації;*
- *квитанція про підтвердження прийняття або неприйняття, або зупинення реєстрації податкової накладної та/або розрахунку коригування – електронний документ, який надсилається платнику податку протягом операційного дня та є підтвердженням прийняття або неприйняття, або зупинення реєстрації податкової накладної та/або розрахунку коригування.*

У ЄРПН наявна функція завантаження та збереження податкових накладних, розрахунку коригування та квитанцій. Також в системі доступна інформація щодо IP-адрес та e-mail, з яких була відправлена податкова накладна.



База даних Національної комісії з цінних паперів та фондового ринку (НКЦПФР) містить інформацію про операції з цінним паперами, про які відзвітували професійні учасники, а саме – торговці цінними паперами та фондові біржі (організатори торгівлі).

Розділ «Біржові контракти, укладені на користь особи» містить інформацію:

- *про укладання фізичною або юридичною особою договорів купівлі/продажу цінних паперів на організованому ринку;*
- *щодо виду фінансового інструменту з яким проводились операції купівлі/продажу на фондовій біржі;*
- *щодо вартості за яку було здійснено купівлі/продаж цінних паперів;*
- *щодо торговця цінними паперами, який представляє інтереси фізичної/юридичної особи при укладанні контрактів на організаторі торгівлі (фондовій біржі).*
- *щодо фондової біржі, на якій проводилась операції купівлі/продажу цінних паперів.*

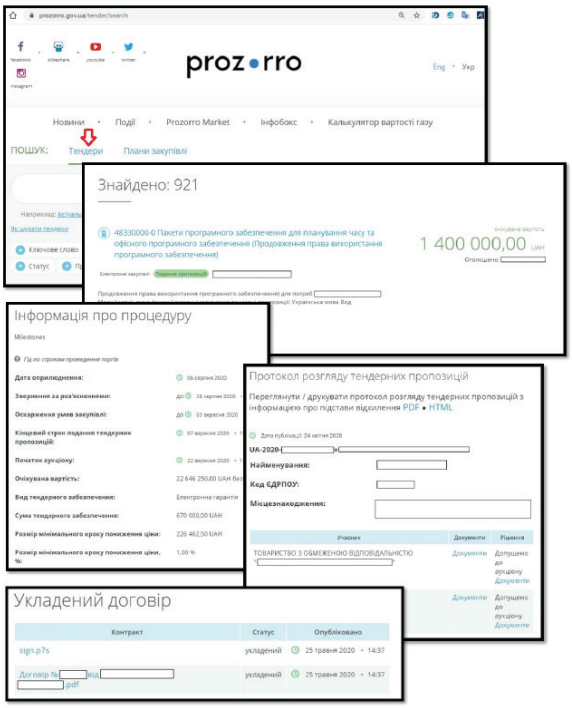
Розділ «Договори з цінними паперами, укладені на неорганізованому ринку» містить інформацію про договори укладені за участю торговця цінними паперами:

- *договори при здійсненні брокерської діяльності;*
- *договори при здійсненні дилерської діяльності.*

Розділ «Належність фізичної особи до посадових осіб емітентів» містить інформацію про всі звіти, які були подані емітентами, в яких фізичні/юридичні особи були зазначені як посадова особа.

Електронна система публічних закупівель PROZORRO

Вебпортал Уповноваженого органу з питань закупівель знаходиться за адресою в мережі Інтернет: www.prozorro.gov.ua.



ІТС «PROZORRO» використовується для отримання інформації з центральної бази даних електронної системи закупівель про річні плани закупівель та безпосередньо самі закупівлі, які були з 01.04.2016 оголошені центральними органами виконавчої влади і замовниками, що здійснюють діяльність в окремих сферах господарювання, та з 01.08.2016 – іншими замовниками.

Пошук планів закупівель. У річному плані закупівель міститься наступна інформація для аналізу в розрізі закупівлі:

- *назва предмета закупівлі;*
- *коди та назви відповідних класифікаторів предмета закупівлі;*
- *код економічної класифікації видатків бюджет;*
- *очікувана вартість предмета закупівлі;*
- *вид закупівлі;*
- *орієнтовний початок проведення процедури закупівлі;*
- *номер плану;*
- *дата публікації;*
- *дата внесення змін;*
- *статус плану;*
- *посилання на оголошену закупівлю;*
- *примітки.*

Пошук закупівель. Вебсторінка в розрізі окремої закупівлі в ІТС «PROZORRO» містить серед іншого наступні блоки інформації:

- *оголошення про проведення;*
- *інформація про замовника;*
- *інформація про процедуру;*
- *інформація про предмет закупівлі;*
- *умови оплати договору;*
- *документація;*
- *роз'яснення до процедури;*
- *вимоги до усунення порушень;*
- *скарги до процедури;*
- *зміни до договору.*

Державний реєстр загальнообов'язкового державного соціального страхування ПФУ. У Реєстрі застрахованих осіб накопичується, зберігається, автоматично обробляється інформація про фізичних осіб, які підлягають загальнообов'язковому державному соціальному страхуванню відповідно до законодавства, та інформація, необхідна для обчислення і призначення страхових виплат за видами загальнообов'язкового державного соціального страхування [15].

Державний реєстр обтяжень рухомого майна. Державна реєстрація обтяжень рухомого майна проводиться з метою забезпечення виконання зобов'язань і захисту прав юридичних і фізичних осіб стосовно рухомого майна та надання в інтересах цих осіб інформації про наявність чи відсутність обтяжень рухомого майна [16].

Єдиний державний реєстр юридичних осіб, фізичних осіб - підприємців та громадських формувань – це єдина державна інформаційна система, що забезпечує збирання, накопичення, обробку,

захист, облік та надання інформації про юридичних осіб, фізичних осіб - підприємців та громадські формування, що не мають статусу юридичної особи [17].

Державний реєстр актів цивільного стану громадян - це державна електронна інформаційна система, яка містить відомості про акти цивільного стану, зміни, що вносяться до актових записів цивільного стану, їх поновлення та анулювання та відомості про видачу свідоцтв про державну реєстрацію актів цивільного стану і про видачу витягів з нього. В даній електронній системі зберігається та обробляється інформація про акти цивільного стану, внесені до них зміни і доповнення, видачу свідоцтва про реєстрацію актів цивільного стану на витягів з Реєстру [18].

Використання Державного реєстру актів цивільного стану громадян дозволяє встановити інформацію щодо факту народження фізичної особи, її походження, усиновлення, позбавлення та поновлення батьківських прав, укладення та розірвання шлюбу, зміни імені та смерті. У базі даних наявна можливість пошуку інформації як за документом (серія, номер), так і за суб'єктом актового запису (ПІБ, дата народження та РНОКПП).

Державний реєстр речових прав на нерухоме майно Міністерства юстиції України. Кримінальний аналітик, використовуючи Державний реєстр речових прав на нерухоме майно, може отримати інформацію щодо речових прав осіб на нерухоме майно (земельні ділянки, житлові та нежитлові приміщення). В реєстраційних даних зафіксовано: адреса нерухомості; реєстраційний номер об'єкту нерухомості; кадастровий номер земельної ділянки; інформація про фізичну або про юридичну особу. В реєстраційних даних зафіксовано: адреса нерухомості; реєстраційний номер об'єкту нерухомості; кадастровий номер земельної ділянки; інформація про фізичну або про юридичну особу. Система дозволяє експортувати отримані в результаті пошуку дані за затвердженим шаблоном.

Автоматизована система виконавчого провадження – це комп'ютерна програма, що забезпечує збирання, зберігання, облік, пошук, узагальнення, надання відомостей про виконавче провадження, формування Єдиного реєстру боржників та захист від несанкціонованого доступу [20].

Єдиний реєстр боржників - це онлайн база даних про боржників, що ведеться з метою оприлюднення в режимі реального часу інформації про невиконані майнові зобов'язання боржників для запобігання відчуженню боржниками майна. Перевірити інформацію: https://erb.minjust.gov.ua/#/search-debtors [21].

Відомості стосовно боржника виключаються з Реєстру одночасно з винесенням постанови про закінчення виконавчого провадження чи в день встановлення виконавцем факту відсутності заборгованості за виконавчими документами про стягнення періодичних платежів.

Єдиний реєстр приватних виконавців України – це сукупність відомостей про приватних виконавців України, які отримали в установленому законодавством порядку посвідчення, та інформації про їх діяльність, яку Міністерство юстиції отримує у процесі реалізації своїх повноважень як державного органу, що здійснює завдання і функції з реалізації державної політики у сфері організації примусового виконання судових рішень і рішень інших органів [22].

Єдиний реєстр довіреностей, посвідчених у нотаріальному порядку. Метою створення Реєстру є профілактика злочинів проти власності шляхом накопичення та використання нотаріусами, органами ДАІ та іншими правоохоронними органами відомостей про посвідчені доручення [23].

Державний земельний кадастр – це єдина державна геоінформаційна система відомостей про землі, розташовані в межах державного кордону України, їх цільове призначення, обмеження у їх використанні, а також дані про кількісну і якісну характеристику земель, їх оцінку, про розподіл земель між власниками і користувачами, про меліоративні мережі та складові частини меліоративних мереж [24].

Геопортал «Ліси України» являє собою веб-сайт та мобільні додатки для доступу й оперування геопросторовою інформацією про ведення лісового господарства. За зверненнями уповноважених органів (#Національної поліції, прокуратури, ДБР, Екоінспекції) було надано доступ до геопорталу «Ліси України» в режимі «перегляд» більш ніж 900 посадовим особам [25].

> *Джерела інформації можуть бути різними і можуть варіюватися в залежності від типу злочину та обставин справи. Ефективний кримінальний аналіз вимагає збору, аналізу та використання цих даних для встановлення фактів та побудови гіпотез задля проведення ефективного розслідування.*

Пошук інформації у державних реєстрах, іноземних реєстрах та базах даних може бути необхідним для різних цілей, таких як встановлення правового статусу підприємства, знаходження інформації про власність, отримання документів чи збір інформації щодо інших суб'єктів.

1. ***Державні реєстри:*** Різні державні реєстри, зберігають повну, або часткову інформацію про компанії, нерухомість, транспортні засоби і т. д. Для пошуку в цих реєстрах, зазвичай, потріб-

но звернутися до відповідного урядового агентства або скористатися онлайн-порталами, які надають доступ до цієї інформації. Наприклад, для пошуку інформації про підприємство в Україні, ви можете відвідати сайт «Єдиного державного реєстру підприємств та організацій» (https://usr.minjust.gov.ua/ua/), а для пошуку інформації щодо земельної ділянки – «Кадастрової карти України» (https://land.gov.ua/).

2. ***Іноземні реєстри:*** Якщо вам потрібно знайти інформацію про компанії або особи, які розташовані за кордоном, ви можете звернутися до відповідних іноземних урядових агентств або скористатися сервісами пошуку компаній, які забезпечують інформацію про підприємства з усього світу. Один з таких сервісів – «Dun & Bradstreet» (https://www.dnb.com/).
3. ***Бази даних:*** Іноді інформацію можна знайти в спеціалізованих базах даних, таких як бази даних для наукових досліджень, патентів, медичних записів і т. д. Для доступу до цих баз даних зазвичай потрібно мати певні дозволи або оплачувати доступ. Наприклад, для наукових досліджень, ви можете скористатися базами даних, такими як PubMed (https://pubmed.ncbi.nlm.nih.gov/), а для патентів - базою даних Патентного відомства США (https://www.uspto.gov/patents).

> *Доступ до інформації у реєстрах та базах даних може бути обмеженим і підлягати правилам конфіденційності та захисту даних.*

СПЕЦІАЛІЗОВАНІ ІНФОРМАЦІЙНІ СЕРВІСИ

Спеціалізоване програмне забезпечення YouControl - це український ресурс, який створює сервіси для аналізу підприємств. Система формує вичерпну інформацію на кожну компанію України на основі відкритих даних, а також відстежує зміни в держреєстрах.

За допомогою онлайн-системи YouControl за лічені секунди можна отримати актуальну (на час запиту) інформацію про будь-яку фізичну чи юридичну особу або приватного підприємця України і щодня дізнаватися про внесені в реєстри зміни [26].

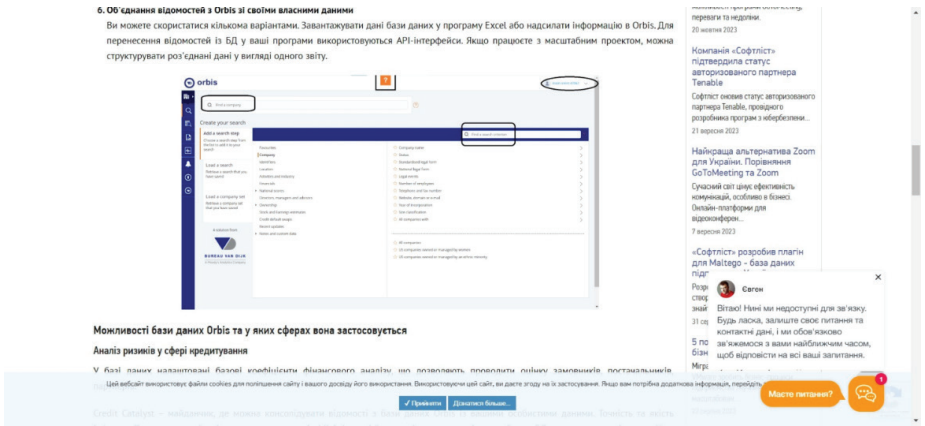
Спеціалізований інформаційний сервіс програмно-пошуковий модуль «Face-check» працює надзвичайно наполегливо, щоб знаходити та індексувати обличчя насильницьких злочинців, ґвалтівників і розбещувачів дітей, сексуальних злочинців, викрадачів, насильників, убивць, злочинців на ґрунті ненависті, грабіжників, членів банди, втікачів, терористів, та шахраїв.

FaceCheck використовує власну технологію штучного інтелекту розпізнавання облич. Глибокі нейронні мережі навчені розпізнавати та підбирати обличчя з різними виразами, під різними кутами, в різних умовах освітлення та закриті бородами, темними окулярами, капелюхами та навіть масками. Щоб отримати найкращі результати, пошукове зображення має бути різким і чітко показувати брови, очі, ніс, рот і лінію щелепи [27].

Спеціалізований інформаційний сервіс програмно-пошукового модулю Vkursi – це онлайн-сервіс для перевірки суб'єктів господарювання, зареєстрованих за законодавством України, перевірки фізичних осіб, моніторингу Державних реєстрів та іншої публічної інформації, а також суміжні технічні можливості [29].

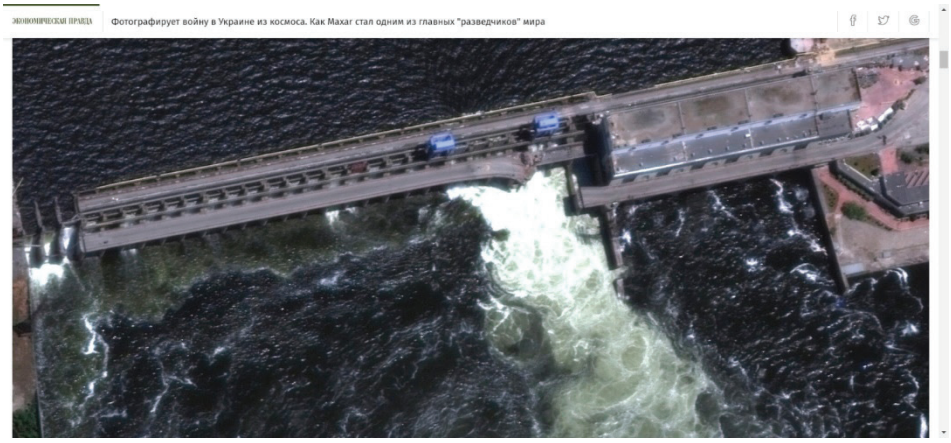
Спеціалізоване програмне забезпечення ArcGis Desktop є програмним забезпеченням, що дозволяє знаходити неявні структури, зв'язку та тенденції даних прихованих в надрах баз даних, електронних таблиць і статистичних пакетів. Крім відображення даних у вигляді точок на карті, ArcGIS дозволяє управляти даними і інтегрувати їх, виконувати розвинений аналіз, моделювати і автоматизувати операційні процеси і виводити результати у вигляді карт професіональної якості [31].

Спеціалізований інформаційний сервіс програмно-пошукового модулю RuAssets виявляє причетність компаній та людей з різних куточків світу до російських та білоруських національних публічних діячів з метою заморожування їхніх рахунків та арешту майна. Також сигналізує про пов'язаність з підсанкційними особами, воєнними терористами та пропагандистами [34].



Спеціалізоване програмне забезпечення Orbis – основний продукт компанії Bureau van Dijk. Це база даних, де користувачі можуть знайти інформацію про підприємство в будь-якій галузі. База регулярно оновлюється та містить актуальні дані щодо організацій. У програмі можна знайти відомості понад 450 мільйонів компаній з усього світу, 45 млн. записів включають деталізовані фі-

нансові дані підприємств. Це об'ємний ресурс із порівнюваною інформацією та оглядом приватних компаній [32].



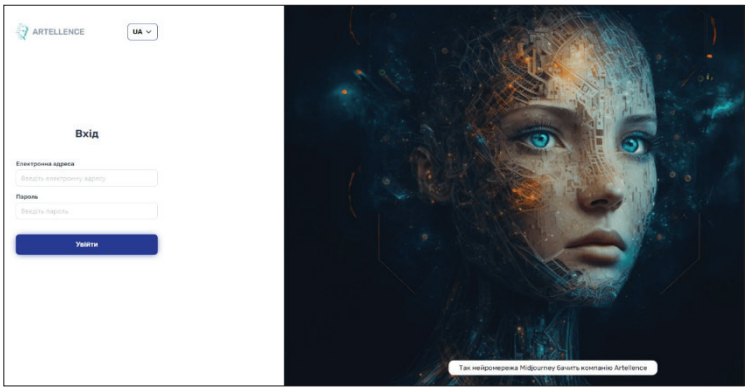
Спеціалізоване програмне забезпечення Maxar. Під час війни в Україні супутникові знімки стали надзвичайно важливим елементом відстеження переміщень військової техніки агресора та фіксування воєнних злочинів країни-терориста. Чи не головний постачальник таких знімків – американська космічна компанія *Maxar Technologies*, яка має на орбіті Землі 90 супутників.

Супутниковий знімок пошкоджень Каховської ГЕС (Джерело: MAXAR)

Це партнерська програма з провідними світовими ЗМІ, які публікують звіти Maxar про війну: від фото братських могил у Бучі та Маріуполі до наслідків теракту РФ в Оленівці та перших знімків після підриву Росією Каховської ГЕС [33]. Компанія займається супутниковими зйомками та виробництвом супутників. Крім того, у неї є проєкт Maxar News Bureau, завдяки якому люди стежать за основними подіями у світі через космос.

Спеціалізований інформаційний сервіс програмно-пошукового модулю Clearview AI надає правоохоронним органам більше інформації та генерує більше можливостей завдяки використанню платформи для проведення розслідувань. Clearview AI включає найбільшу з відомих баз даних, що містить понад 30 мільярдів зображень обличь, отриманих із загальнодоступних веб-ресурсів, включаючи новинні ЗМІ, веб-сайти з фотографіями, загальнодоступні соціальні мережі та багато інших відкритих джерел [35].

Спеціалізований інформаційний сервіс програмно-пошукового модулю Big Data People (Artellence). Технологія штучного інтелекту (ШІ) постійно вдосконалюється і може виконувати набагато більше функцій. ІТ-компанія Artellence розробила нейронні мережі для аналізу тексту, пошуку по профілю обличчя, а також алгоритми очищення та структурування великих даних. Це дозволяє виявляти людей, які можуть завдати шкоди нашій країні на різних рівнях. Основним продуктом є BigDataPeople, який за лічені секунди аналізує величезні обсяги даних і генерує рекомендації та корисну інформацію [36].



Банки даних Інтерполу. Використання банків даних Інтерполу є однією із форм міжнародного поліцейського співробітництва. Банки даних Генерального секретаріату Інтерполу створені з метою забезпечення всебічної взаємодії правоохоронних органів держав-членів Інтерполу. З банків даних Інтерполу з використанням інформаційної системи Інтерполу може бути отримано:

- *інформацію* про осіб;
- *інформацію* про транспортні засоби, які перебувають у розшуку;
- *інформацію* про плавзасоби, які перебувають у розшуку;
- *інформацію* про викрадені, втрачені, підроблені, недійсні документи, що підтверджують громадянство, посвідчують особу чи її спеціальний статус;
- *інформацію* про твори мистецтва / культурні цінності;
- *інформацію* про вогнепальну зброю;
- *сліди рук*, вилучені з місць вчинення злочину;
- *дактилоскопічну* карту;
- *ДНК-профілі*;
- *зображення* дітей, які зазнали сексуальної експлуатації;
- *інші дані* (у разі створення в Генеральному секретаріаті Інтерполу банків даних інших категорій інформації).

У Генеральному секретаріаті Інтерполу створені та функціонують наступні банки даних:

1. Особи:

1) банк даних «Особи» (ASF Nominal database) – містить інформацію про відомих міжнародних злочинців, зниклих осіб та невпізнані трупи з історією їх злочинів, фотографіями, відбитками пальців тощо.



Крім того, Генеральний секретаріат за допомогою системи I-24/7 надає доступ до банку даних циркулярних повідомлень Інтерполу. У зазначеному банку даних міститься інформація про усі зазначені циркулярні повідомлення в електронному вигляді.

Департамент міжнародного поліцейського співробітництва (ДМПС) Національної поліції на підставі отриманого від правоохоронного органу України запиту чи звернення забезпечує використання інформаційної системи Інтерполу шляхом надсилання запиту про публікацію Генеральним секретаріатом Інтерполу оповіщень:

Червоне оповіщення (RED NOTICE) – *«розшукується»* – оповіщення щодо осіб, які розшукуються з метою їх затримання, арешту, обмеження свободи пересування та подальшої видачі (екстрадиції) в Україну.

Синє оповіщення (BLUE NOTICE) – *«встановлення місцезнаходження»* – оповіщення щодо осіб, які становлять інтерес для правоохоронних органів України в рамках кримінальних проваджень та/або оперативно-розшукових справ, з метою: отримання інформації про особу; встановлення місцезнаходження особи; ідентифікації особи.

Зелене оповіщення (GREEN NOTICE) – *«попередження»* – оповіщення з метою попередження компетентних органів іноземних держав про злочинну діяльність певних осіб («професійних» злочинців, які діють на території декількох країн).

Чорне оповіщення (BLACK NOTICE) – *«невпізнаний труп»* –оповіщення з метою встановлення особи за невпізнаним трупом.

Жовте оповіщення (YELLOW NOTICE) – *«зниклий безвісти»* –оповіщення з метою встановлення місцезнаходження особи, зниклої безвісти, або для ідентифікації особи, яка не може повідомити відомості про себе.

Пурпурне оповіщення (PURPLE NOTICE) – *«спосіб злочину»* –оповіщення з метою: попередження про способи вчинення злочинів, предмети, методи і способи приховування злочинів; запиту інформації, яка може сприяти досудовому розслідуванню злочинів.

Помаранчеве оповіщення (ORANGE NOTICE) – *«безпосередня загроза»* – оповіщення з метою попередження про подію, особу, предмет, спосіб вчинення злочину, що становлять реальну загрозу публічній безпеці та порядку і можуть завдати істотної шкоди майну чи громадянам.

Оповіщення про викрадені культурні цінності – *«культурні цінності»* – оповіщення з метою встановлення місцезнаходження викрадених творів мистецтва або інших предметів, що становлять культурну цінність, або для ідентифікації таких об'єктів.

2) банк даних порнографічних зображень, створених із залученням неповнолітніх (INTERPOL Child Abuse Image database), дозволяє ідентифікувати зображення порнографічного характеру за «авторством» та місцем розміщення в мережі Інтернет. *Міжнародний банк даних зображень та відео щодо сексуальної експлуатації дітей (ICSE)* – це інструмент розвідки та розслідування, який дозволяє спеціалізованим слідчим ділитися даними про випадки сексуального насильства над дітьми. Використовуючи програмне забезпечення для порівняння зображень та відео, слідчі можуть миттєво встановити зв'язок між жертвами, зловмисниками та їх місцезнаходженням.

2. Криміналістика

Відбитки пальців, профілі ДНК та розпізнавання осіб можуть зіграти вирішальну роль у розкритті злочинів, оскільки вони можуть встановити зв'язок між особами та/або місцями вчинення злочинів, зокрема:

1) банк даних відбитків пальців рук (Fingerprints database). Уповноважені користувачі в країнах-членах можуть переглядати, подавати та перехресно перевіряти записи в банку даних відбитків пальців за допомогою *автоматизованої системи ідентифікації відбитків пальців (AFIS).*

2) банк даних ДНК-профілів (DNA Profiles database) – містить інформацію про профілі ДНК, вилучені з місць вчинення злочинів на території держав-членів Інтерполу та від злочинців.

3) I-Familia. Метою I-Familia є виявлення зниклих безвісти осіб у всьому світі за допомогою відповідності сімейної ДНК. Його рушійний принцип – гуманітарний: возз'єднати близьких або закрити справи.

4) система розпізнавання обличчя забезпечує спеціальну платформу для зберігання та перехресної перевірки зображень з метою ідентифікації втікачів, зниклих безвісти осіб та осіб, що представляють оперативний інтерес. Система розпізнавання осіб Interpol Facial Recognition System (IFRS) містить зображення обличчя, отримані з більш ніж 179 країн, що робить її унікальною глобальною базою даних про злочини. Робота з якісними зображеннями має вирішальне значення. Стандартна фотографія паспорта ІКАО є оптимальною, оскільки це фронтальне зображення предмета, яке має рівномірне освітлення на обличчі та нейтральний фон.

3. Банк даних викрадених/втрачених документів

містить інформацію про викрадені/втрачені ідентифікаційні документи, а також викрадені/втрачені бланки адміністративних документів, які використовуються для ідентифікації об'єктів, зокрема:

1) викрадені та загублені проїзні документи (SLTD) – зберігаються дані про втрачені, викрадені та анульовані проїзні документи (паспорти, посвідчення особи, пропуски ООН або візові штампи, включаючи викрадені бланки проїзних документів);

2) викрадені адміністративні документи (SAD) – містить дані про викрадені офіційні документи, які служать для ідентифікації об'єктів (документи про реєстрацію транспортних засобів, сертифікати оформлення для імпорту/експорту тощо);

3) підроблені документи – цифрова бібліотека сповіщень Interpol (Document (Dial-Doc)) – дозволяє країнам ділитися на світовому рівні попередженнями, що готуються на національному рівні, щодо нових виявлених форм підробки документів;

4) порівняння справжніх та фальшивих документів – електронна система документації та інформації про мережі розслідувань (Едісон) містить зображення, описи та захисні елементи справжніх проїзних документів та документів, що посвідчують особу, виданих країнами та міжнародними організаціями, щоб допомогти виявити підробку.

4. Викрадене майно

Глобальні банки даних Інтерполу допомагають правоохоронним спільнотам у виявленні викрадених речей та збільшують шанс на їх повернення, зокрема:

1) *банк даних викрадених транспортних засобів (ASF Stolen Vehicles database)* – містить інформацію про транспортні засоби, викрадені на території держав-членів Інтерполу.

2) банк даних викрадених плавзасобів (ASF Stolen Vessels database) – банк даних викрадених плавзасобів служить централізованим інструментом для відстеження та встановлення викрадених плавзасобів та двигунів до них;

3) банк даних викрадених творів мистецтва (ASF Stolen Works of Art) – містить інформацію щодо творів мистецтва, предметів антикваріату, інших культурних цінностей, викрадених на території 134 держав-членів Інтерполу.

5. Торгівля вогнепальною зброєю

Три потужні інструменти допомагають країнам-членам Інтерполу збирати й аналізувати інформацію, яка може бути отримана як всередині так і ззовні країни, з метою запобігання та розкриття злочинів, пов'язаних із вогнепальною зброєю, а саме:

1) Довідкова таблиця вогнепальної зброї Інтерполу «Ідентифікація вогнепальної зброї» являє собою інтерактивний онлайн-інструмент, який забезпечує стандартну методику для виявлення і опису вогнепальної зброї більш точно, таким чином вони можуть бути простежені в транскордонних дослідженнях;

2) автоматизована система «Розшук вогнепальної зброї» – система управління документацією Інтерполу про незаконне озброєння та управління відстеженням зброї *(iARMS),* що забезпечує централізовану платформу для звітності, запитів та трасування втраченої, викраденої зброї, незаконної торгівлі або контрабанди вогнепальної зброї правоохоронними органами у всьому світі;

3) Балістична інформаційна мережа Інтерполу (IBIN) «Порівняння балістичних даних» – єдина масштабна платформа для міжнародного обміну та порівняння балістичних даних, що дозволяє здійснювати пошук зв'язків між злочинами в різних країнах.

6. Мережі організованої злочинності

Метою банку даних «Мережі організованої злочинності» є покращення збору та обміну розвідувальними даними, підтримка розслідувань та кращий аналіз злочинних мереж, що може призвести до ідентифікації та арешту їх керівників та фінансистів.

7. Морське піратство

Банк даних «Морське піратство» зберігає інформацію, пов'язану з випадками піратства та збройного пограбування на морі, включаючи дані про фізичних осіб, номери телефонів, адреси електронної пошти, випадки піратства, місцезнаходження, підприємства та фінансову інформацію.

Використання інформаційної системи Інтерполу правоохоронними органами України здійснюється відповідно до порядку, встановленого *Інструкцією про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол* [38], у формі надсилання запиту/звернення до уповноваженого підрозділу або у формі прямого доступу.

Отримання інформації або перевірка тих чи інших відомостей за банками даних Інтерполу здійснюється:

- *безпосередньо*, в режимі on-line – через комунікаційну систему Інтерполу I-24/7 (банки даних щодо осіб, транспортних засобів, документів, творів мистецтва);
- *шляхом надсилання запиту* до Генерального секретаріату Інтерполу (банки даних ДНК, порнографічних зображень, відбитків пальців).

У 2015 році в Україні була впроваджена технологія підключення до *комунікаційної системи Інтерполу FIND* (Fixed INTERPOL Network Database – фіксована мережна бази даних Інтерполу), що передбачає інтеграцію комунікаційної мережі Інтерполу з комунікаційними системами національних правоохоронних органів [39].

Аналітики підрозділів кримінального аналізу мають доступ до комунікаційної системи Інтерполу FIND, зокрема до підсистем: особи, транспортні засоби, втрачені (загублені) проїзні документи.

ВИКОРИСТАНІ ДЖЕРЕЛА:

1. Положення про Департамент кримінального аналізу Національної поліції України: наказ Національної поліції України від 29 груд. 2019 р. № 1354.
2. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку пріоритетних електронних інформаційних ресурсів її суб'єктів: постанова Кабінету Міністрів України від 14 листоп. 2018 р. № 1024 (в редакції постанови Кабінету Міністрів України від 15 серп. 2023 р. № 866).
3. Про затвердження Положення про Департамент інформаційно-аналітичної підтримки Національної поліції України: наказ Національної поліції України від 31 січн. 2020 р. № 77 (зі змінами від 13 листоп. 2020 р. № 885).
4. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України»: наказ МВС від 03 серп. 2017 р. № 676 (зі змінами від 14 лют. 2022 р. № 122).
5. Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС: наказ МВС України від 20 жовт. 2017 р. № 870. URL: https://zakon.rada.gov.ua/laws/show/z1433-17/print
6. Деякі питання ведення обліку відомостей про притягнення особи до кримінальної відповідальності та наявності судимості: наказ МВС України від 30 берез. 2022 р. № 207 (зі змінами від 22 берез. 2023 р. № 227).
7. Деякі питання функціонування Єдиного державного реєстру транспортних засобів: наказ МВС України від 06 лист. 2020 р. № 779.
8. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Гарпун» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України»: наказ МВС від 13 черв. 2018 р. № 497.
9. Про затвердження Положення про інтегровану міжвідомчу інформаційно-телекомунікаційну систему щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон: наказ АДПС, ДМС, ДПА, МВС, МЗС, Мінпраці та соцполітики, СБУ, СЗР України від 03 квіт. 2008 р. N 284/287/214/150/64/175/266/75.
10. Спеціальне програмне забезпечення допомагає ДМС ефективніше працювати з іноземцями та особами без громадянства. URL: https://dmsu.gov.ua/news/dms/9043.html
11. Порядок організації доступу до інформаційних ресурсів під час інформаційної взаємодії між Міністерством внутрішніх справ України, Державною міграційною службою України та Державною прикордонною службою України: наказ МВС від 26 верес. 2013 р. № 920.
12. У рамках проекту «Безпечне місто» запущено новий аналітичний модуль відеоспостереження, що прискорить пошук правопорушників. URL: https://kyivcity.gov.ua/news/u_ramkakh_proektu_bezpechne_misto_zapuscheno_noviy_analitichniy_modul_videosposterezhennya_scho_priskorit_poshuk_pravoporushnikiv/

13. Порядок електронної інформаційної взаємодії Офісу Генерального прокурора та Міністерства внутрішніх справ України: Наказ Генерального прокурора, Міністерства внутрішніх справ України 22 лист. 2021 р. № 371/846.
14. Про затвердження Порядку ведення Єдиного державного реєстру судових рішень: затверджено Рішенням Вищої ради правосуддя 19 квіт. 2018 р. № 1200/0/15-18 (із змінами).
15. Положення про реєстр застрахованих осіб Державного реєстру загальнообов'язкового державного соціального страхування: Постанова правління Пенсійного фонду України 18 червн. 2014 р. № 10-1 (у редакції постанови правління Пенсійного фонду України від 27 берез. 2018 р. № 8-1).
16. Порядок ведення Державного реєстру обтяжень рухомого майна: постанова Кабінету Міністрів України від 5 лип. 2004 р. № 830.
17. Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань: Закон України від 15 трав. 2003 р. № 755-IV. Відомості Верховної Ради України, 2003, № 31-32, ст.263.
18. Про державну реєстрацію актів цивільного стану: Закон України від 01 лип. 2010 р. № 2398-VI. Відомості Верховної Ради України, 2010, № 38, ст. 509.
19. Кіреєва О.С., Крутік Ю.В., Махлай О.М., Треус А.С. Основи кримінального аналізу: теорія та практика застосування в оперативних підрозділах Державної прикордонної служби України: навчальний посібник / за заг. ред. О.С. Кіреєвої. Хмельницький: Вид-во НАДПСУ, 2022. 360 с.
20. Про затвердження Положення про автоматизовану систему виконавчого провадження: наказ Міністерства юстиції України від 05 серп. 2016 р. N 2432/5.
21. Департамент Державної виконавчої служби. URL: https://minjust.gov.ua/ddvs/reiestr_borzhnykiv
22. Про затвердження Порядку формування і ведення Єдиного реєстру приватних виконавців України: наказ Міністерства юстиції України від 05 серп. 2016 р. N 2431/5.
23. Єдиний реєстр довіреностей, посвідчених у нотаріальному порядку. URL: https://minjust.gov.ua/m/str_2351
24. Про Державний земельний кадастр: Закон України від 07 лип. 2011 р. № 3613-VI.
25. Геопортал Ліси України. URL: https://forestry.org.ua/
26. YouControl — це українська команда, яка створює сервіси для аналізу підприємств. URL: https://youcontrol.com.ua/about_us/
27. Face-check. URL: https://facecheck.id/
28. i2 Analyst's Notebook. URL: https://rdtex.ua/i2-software/solutions-based-on-i2-analyst-s-notebook/
29. Публічний договір. Умови користування. URL: https://vkursi.pro/opportunity/publiccontract
30. Power BI. URL: https://uk.wikipedia.org/wiki/Power_BI
31. ArcGIS Desktop. URL: https://esri.ua/sarticle.php?id=2
32. Огляд бази даних ORBIS: як швидко дізнатися актуальну інформацію про компанію. URL: https://ua.softlist.com.ua/articles/obzor-bazy-dannykh-orbis-kak-bystro-uznat-aktualnuyu-informaciyu-o-kompanii/
33. Фотографує війну в Україні з космосу. Як Maxar став одним з головних «розвідників» світу. URL: https://www.epravda.com.ua/publications/2023/06/7/700909/
34. YouControl створив інструмент для виявлення прихованих російських і білоруських активів. URL: https://youcontrol.com.ua/news/russianassets/
35. 10 мільярдів фото і система розпізнавання: Україна отримала доступ до бази Clear view AI. URL: https://www.ukrinform.ua/rubric-technology/3429032-10-milardiv-foto-i-sistema-rozpiznavanna-ukraina-otrimala-dostup-do-bazi-clearview-ai.html
36. Федоров М. Технічні інновації України, народжені війною. URL: https://english.nv.ua/opinion/ukraine-s-tech-innovations-born-of-war-opinion-50360587.html
37. Face ID Демо. Спробуйте демо системи розпізнавання та порівняння облич за фото. URL: https://evergreens.com.ua/ua/box-products/face-id/demo.html.
38. Інструкція про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол: наказ МВС, Офісу Генерального прокурора, НАБУ, СБУ, ДБР, Мінфіна, Мінюста від 17 серп. 2020 р. № 613/380/93/228/414/510/2801/5.
39. Довідка про основні результати службової діяльності Національного центрального бюро Інтерполу в Україні у 2022 році. URL: https://dostup.pravda.com.ua/request/104660/response/372851/attach/3/01.2023.pdf

НАПРЯМИ ТА ОСОБЛИВОСТІ ЗАСТОСУВАННЯ КРИМІНАЛЬНОГО АНАЛІЗУ В УМОВАХ ВОЄННОГО СТАНУ

DOI: https://doi.org/10.36486/978-966-2310-66-5-15

Людина, яка хоч раз вхопила кішку за хвіст, знає про котів значно більше, ніж та, яка тільки читала про них, але ніколи не бачила.

Марк Твен

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

Роман Бутко
Ігор Сальніков
Вадим Петров
Андрій Сивун
Ігор Шишкін

СУЧАСНІ ТЕНДЕНЦІЇ ТА НОВАЦІЇ СИСТЕМНОГО РОЗВИТКУ КРИМІНАЛЬНОГО АНАЛІЗУ В НПУ

Служба кримінального аналізу пройшла велику трансформацію за короткий проміжок часу. На жаль, певним поштовхом для цього стало і повномасштабне вторгнення російської федерації.

Слід зазначити, що у 2016 році, з якого веде початок кримінальний аналіз в Національній поліції, злочинність уже користувалась всіма перевагами сучасних технологій, саме тому перед поліцією постало завдання пошуку гідного системного рішення. Одним із таких рішень стало розбудова напряму кримінального аналізу. Перший прецедент – це створення відділу, де було лише 5 аналітиків. Мови про створення повноцінного підрозділу не було [1].

У 2017 році вже самостійний підрозділ кримінального аналізу увійшов до складу кримінальної поліції, почали активніше впроваджуватися новітні підходи в роботі та розкритті злочинів. 2019 рік став етапом переоцінки наявного досвіду та створення перших 5 територіальних підрозділів. Пандемія коронавірусу SARS-CoV-2 навчила аналітиків працювати дистанційно, не втрачаючи якості в роботі. Цей досвід також став у нагоді під час повномасштабного вторгнення [2]. У 2022 році команда аналітиків збільшилася до 173 працівників. Попит на продукти кримінального аналізу збільшився у декілька разів. Аналітики посіли важливе місце у структурі поліції.

2022 року розпочалася розбудова столичної служби кримінального аналізу, створення в кожному районному управлінні поліції Києва секторів з трьох аналітиків [3]. Щодня аналітики почали отримувати значну кількість інформації з «землі» та майже на 100 % перекрили вирішення робочих питань на місцевому рівні. А на початку 2023 року цей досвід почав масштабуватися на всю державу.

На сьогодні підрозділи кримінального аналізу функціонують у кожному з 25 обласних управлінь поліції, а також створено 35 підрозділів на місцевому рівні (сектор кримінального аналізу відділу кримінальної поліції районного управління поліції). Кількість працівників підрозділів кримінального аналізу на всіх рівнях складає більше 400 осіб, майже 70% з них це аналітики-практики.

> *Інституційна розбудова спроможностей кримінального аналізу протягом усього періоду супроводжувалася активною співпрацею з міжнародними партнерськими організаціями та адаптацією набутого досвіду. Ці складові лягли в основу реформування та реорганізації служби, розвитку її структури.*

Пріоритети діяльності підрозділів кримінального аналізу визначені з урахуванням успішних зарубіжних моделей та вимогами сьогодення. Крім інформаційно-аналітичного супроводження розкриття злочинів загальнокримінальної спрямованості, аналітики зосереджені на проведенні аналітичних досліджень у сфері ліквідації економічного підґрунтя злочинної діяльності, зборі доказової бази воєнних злочинів країни-агресора, а також проведенні відеоаналітичних досліджень.

За сприяння й координації Міністерства внутрішніх справ аналітики Національної поліції розбудовують партнерство зі спорідненими службами системи МВС. Зокрема, йде активна співпраця з Центром стратегічного аналізу та прогнозування МВС України, а також Управлінням інформацій-

но-аналітичного забезпечення та кримінального аналізу Департаменту оперативно-розшукової діяльності Адміністрації Державної прикордонної служби України.

Зокрема, для ефективної взаємодії та стандартизованого підходу до виконання завдань, спеціально створеною робочою групою вживаються заходи з уніфікації аналітичних продуктів, організується оперативний обмін інформацією.

> *Основною метою є розширення можливостей кожного аналітика та служби в цілому. Пріоритетним є також раціональний розподіл аналітичних ресурсів.*

Служба кримінального аналізу налагодила взаємодію з міжнародними партнерами та разом з ними організувала постійний навчальний процес. Організовано навчальні заходи, стажування та курси. Аналітиками взято участь у значній кількості зустрічей на міжнародному рівні з представниками провідних правоохоронних організацій Європейського союзу.

Водночас умови, у яких живе суспільство, спонукали до створення підрозділу ситуаційного аналізу. Ідея була у тому, щоб один аналітик володів оперативною обстановкою у регіоні 24/7. На цей підрозділ також покладається функція комунікації з іншими службами та фіксація наслідків обстрілів. Під час реєстрації або виявленні злочину аналітик відразу виконує 5-7 заздалегідь визначених аналітичних завдань та швидко передає інформацію оперативним працівникам для розкриття чи документування злочину. Такий «проактивний» підхід до використання аналітика підрозділу кримінального аналізу був високо оцінений і на регіональному рівні.

> *Окремо у структурі підрозділів кримінального аналізу була виділена лінія, відповідальна за стратегічний аналіз - SOCTA.*

Це стало можливим після переосмислення пріоритетів, а також оцінки важливості аналізу не лише для конкретного правоохоронного органу, а й для держави в цілому [4]. Кожен аналітик закріплений за певною лінією аналізу. Співробітники, що займаються прогнозним аналізом, зорієнтовані на дослідження можливих тенденцій розвитку злочинності як в середині країни, так і за її межами.

> *Одним із останніх нововведень стала також розбудова відділу, відповідального за відео- та фотоаналіз [5].*

На сьогоднішній день підрозділи кримінального аналізу щодня на професійному рівні користуються системами відеоспостереження та аналізують сотні терабайт відеоматеріалів. Підрозділи кримінального аналізу розкрили весь свій накопичений потенціал у секторі відеоаналітики саме з повномасштабним вторгненням – а це аналіз великих масивів відео, геопросторовий аналіз, аналіз маршрутів руху, у тому числі військової техніки ворога, розпізнання воєнних злочинців, мародерів, диверсантів, покращення відеоматеріалів, спростування дезінформації, що набувала суспільного резонансу та сіяла деморалізацію і паніку (ІПСО).

Додатковим поштовхом було надходження надвеликої кількості відео для аналізу. Кількість відеоматеріалу на одного аналітика з початку війни зросла у геометричній прогресії. Тільки Департамент кримінального аналізу проаналізував більше 200 терабайтів матеріалів щодо воєнних та інших злочинів. Аналітики показали ефективність результатів своєї роботи, а тому потреба в аналітичних продуктах зросла.

Наразі в Департаменті кримінального аналізу ***сформовано новий відділ – відеоаналітичних досліджень***, який не просто займається профільною аналітикою, а спирається на аналіз великих за обсягом відеоматеріалів, здійснює розпізнання виявлених на відео суб'єктів та об'єктів, встановлення та аналіз маршруту руху, покращення якості відео- та фотозображень, візуалізацію результатів роботи з метою їх подальшого використання [6].

Для аналізу великих за обсягом відеоматеріалів використовуються спеціалізовані програмно-аналітичні платформи, що дають змогу швидко аналізувати великі масиви відео. Дані платформи спеціалізуються на індексації завантажених відеоматеріалів з подальшим розбиттям їх на певні класи об'єктів, з якими аналітики в подальшому працюють.

Аналітики здійснюють ***постійний OSINT-аналіз*** для виявлення публікацій, що можуть викликати суспільний резонанс, з установленням причетних до них осіб. Зазвичай, підрозділи кримінального аналізу перші виявляють дані публікації та відпрацювавши їх, уже надають готові матеріали, що можуть принести результати.

За допомогою унікальних ресурсів, єдиних інтеграційних платформ регіональних систем відеоспостереження та знань аналітиків проводиться детальний аналіз пересування осіб злочинців, потерпілих, транспортних засобів та інших об'єктів по всій території України.

З розвитком технологій штучного інтелекту аналітики отримали змогу здійснювати покращення відеоматеріалів, особливо здійснених у темну пору доби. Це питання завжди було актуальним, адже більшість злочинів учиняються в нічний час, злочинці розуміють, що можуть використовувати це як перевагу, а тому отримання для правоохоронних потреб ресурсів, які дозволяють із цим боритися, очікувало свого часу. Окрім відеоматеріалів, покращенню піддаються і фотоматеріали. Оскільки сам напрям покращення вважається новим, виникають і перші проблеми – такі як опрацювання відеоматеріалів, отриманих з камер відеоспостереження з можливістю нічного бачення, або просто статичних камер.

Геопросторовий аналіз не новий напрям аналітики, особливо для підрозділів Національної поліції, але починаючи з лютого 2022 року, необхідність у ньому почала зростати в геометричній прогресії. Аналітики по всій Україні почали відпрацьовувати OSINT-джерела для виявлення місць розташування ворожої техніки, особового складу армійських підрозділів рф, місць їх дислокації, а також пошуку місць ворожих ракетних ударів. Зазвичай, для проведення даного виду аналізу використовуються OSINT-ресурси, але інколи виникає потреба використання ресурсів з можливістю отримання супутникових знімків на певній місцевості та у конкретну дату.

Потрібно зазначити, що всі вище перелічені нові напрями аналітики майже ніколи не застосовуються окремо, *відеоаналітичні дослідження – це комплекс заходів, який у собі охоплює якнайбільшу кількість методик та ресурсів для отримання швидкого, повного та ефективного результату*.

Останнім етапом аналізу завжди є ***візуалізація результатів*** роботи. За результатами проведених аналітичних заходів вся інформація узагальнюється у відповідному форматі для подальшої її реалізації замовниками або особами, які отримають аналітичний продукт. Уся отримана та опрацьована в результаті аналітичних досліджень інформація повинна бути викладена у зрозумілій для замовника формі. Цією формою може бути відеоряд, схема, аналітичний звіт або будь-який інший аналітичний документ [5].

Ще одним пріоритетом розбудови служби є успішна інтеграція українського кримінального аналізу у світовий аналітичний простір. З цією метою

> *в Департаменті створено відділ міжнародного співробітництва з обміну аналітичною інформацією.*

Вимоги до таких аналітиків високі – крім професійних знань і навичок від них вимагається вільне володіння іноземною мовою, а також основами міжнародного права та економіки [7].

Таким чином створюється своєрідний інститут офіцерів зв'язку у сфері розвідувальної аналітики, передусім з пошуку закордонних активів українського криміналітету та російського сліду у вітчизняній економіці.

Безперечно війна вплинула на функції та завдання підрозділів кримінального аналізу. Аналітик працює з матеріалами не лише звичного поліцейського формату, а й воєнних злочинів, пошуку активів ворога для відбудови України.

> *Аналітик - це не просто офіцер, а особа, що робить рішення оперативних підрозділів та слідчих обґрунтованими та ефективними. Він здатний зіставити шматочки інформації, звернути увагу на деталі. Під час війни він має діяти у незвичному полі.*

Мотив злочину часто не містить логічного пояснення, жертви давно були змушені залишити країну, докази перебувають на окупованій території, а злочинці відчувають безкарність. Окрім цього, аналітик постійно має справу з великим обсягом повідомлень про злочини.

Від нього вимагається повна обізнаність у техніці, позивних, різновидах військової форми та інших деталях військових, причетних до злочину.

При розслідуванні воєнних злочинів аналітик забезпечує:

- *максимальне охоплення ЗМІ для збору інформації, а також інших джерел, які висвітлюють воєнні події, в тому числі і ворожі, матеріали з попередніх конфліктів, а також їх збереження;*
- *документування відомостей і фактів, особливо в частині переміщення військових формувань та їх фіксації на певній території;*
- *фокусування на певній ділянці бойових дій, особливо під час гарячих фаз через масштабність подій та швидку зміну оперативної обстановки;*
- *обізнаність у використанні новітніх методів аналізу, у тому числі супутникових знімків.*

За умови забезпечення переліченого, аналітик стає майже незамінним при розслідуваннях воєнних злочинів.

Перед аналітиками постали нові завдання, які були пов'язані з наступною аналітичною діяльністю:

- *аналіз інформації з відкритих джерел про військовослужбовців агресора, які діяли на території України, в тому числі моніторинг інформації про рух або скупчення військових формувань на певній території країни;*
- *опанування новітніх методів аналізу, в тому числі картографування та геопросторовий аналіз;*
- *збір та аналіз інформації про процеси, які відбуваються на окупованих територіях;*
- *аналіз інформації про громадян України, які можуть бути причетні до колабораційної діяльності;*
- *протидія інформаційно-психологічним операціям ворога (ІПСО);*
- *боротьба з поширенням інформації про переміщення, рух або розташування Збройних Сил України [8].*

У тісній співпраці з міжнародними командами аналітиків, продемонстровано високі результати роботи аналітиків ДКА.

Завдяки скрупульозній роботі вдалося встановити осіб, причетних до обстрілу житлових будинків у місті Чернігові навесні 2022 року. Після встановлення азимута падіння снарядів було вирахувано декілька вірогідних місць запуску снарядів.

Коли території були деокуповані, поліцією були проведені опитування місцевих мешканців на предмет розміщення військових формувань у їх населених пунктах. У результаті проведених заходів визначені артилерійські формування, причетні до обстрілів. Далі, шляхом перевірки інформації з відкритих джерел, були ідентифіковані причетні до злочину особи.

Другий приклад залучення аналітиків стосується воєнних злочинів, учинених на території одного з населених пунктів Київської області.

Завдяки аналізу інформації про техніку, яку використовували росіяни, були виявлені матеріали, що підтверджують участь військового формування на території інших напрямів, починаючи з 2014 року. Це дало підґрунтя для ідентифікації можливих військовослужбовців, а також їх командирів, які безпосередньо віддавали наказ.

У третьому випадку першочергово було отримано інформацію про участь іноземця у військових формуваннях рф, що діють на території України. Завдяки найпростішому OSINT-аналізу були отримані першочергові відомості для ідентифікації такої особи. У подальшому вдалося встановити підрозділ, де іноземець проходив службу, перевірено причетність до воєнних злочинів аналогічного спрямування, перевірено його спільників.

Кожне повідомлення про злочин відпрацьовано та структуровано за декількома десятками параметрів. Визначені військові формування, ймовірні позивні, місце вчинення злочину. За можливістю проаналізовано військову техніку, яка перебуває у розпорядженні частини. Зібрано відомості з соціальних сторінок. Додано відомості від потерпілих, у тому числі і тих, хто виїхав з країни.

Уся вказана інформація структурована в декількох десятках графіків та даних для ефективного пошуку як за місцем вчинення злочину, так і за параметрами злочинця чи свідченнями жертви.

Саме така основа із зібраних даних дає можливість проводити аналіз навіть у випадках складних та великих за обсягом розслідувань.

З початку широкомасштабного вторгнення рф, до поліції надходять тисячі повідомлень про зникнення громадян. До них належать повідомлення родичів, які втратили зв'язок з рідними, а також повідомлення про зникнення людей на окупованих територіях.

Ураховуючи викладене, питання розшуку безвісти зниклих є одним із пріоритетних напрямів роботи, у якій аналітики беруть активну участь. З використанням OSINT, програм розпізнавання та інших аналітичних інструментів здійснюється відпрацювання кожної зниклої особи на предмет зв'язків та контактів, через які можна встановити її місце перебування.

> *Установлення безвісті зниклих під час воєнних дій – це аналітичне дослідження одне з найскладніших для відпрацювання як класичними методами, так і за допомогою аналітики.*

Дослідження такого змісту нагадують роботу з неструктурованим масивом інформації великого обсягу. Повідомлення про зникнення рахуються тисячами і варіюються від повідомлень родичів, які втратили зв'язок з рідними, до зникнення осіб у ході окупації певних територій.

Інколи злочинці намагаються скористатися воєнним часом для приховання та інсценування вбивств чи грабежів. Таким чином зловмисники намагаються перекласти відповідальність на інших осіб, яких, на їхню думку, практично неможливо відстежити.

Тому приділяється максимальна увага кожній справі про зникнення і відразу приступають до комплексу розшукових та аналітичних заходів. Така робота безпосередньо пов'язана з накопиченням та узагальненням величезного обсягу даних про зниклих осіб.

Кожна зникла людина відпрацьовується на предмет зв'язків та контактів, через які можна встановити її місце перебування. Проводиться відповідний моніторинг ЗМІ. Кожний випадок при цьому індивідуальний, але за кожним повідомленням стоїть доля людини.

> *На сьогодні можна констатувати, що за 2022 рік та 10 місяців 2023 року аналітики взяли участь у розкритті понад 25 тисяч злочинів, більшість з яких особливо тяжкі.*

При використанні аналітичних інструментів значна увага приділяється дотриманню європейських стандартів захисту персональних даних GDPR [9]. Наші аналітики, як ніхто інший, розуміють важливість євроінтеграції в поліції та загальному курсі держави.

> *У сучасних умовах розслідування злочинів економічної спрямованості набуває особливого значення, оскільки економічні злочини можуть мати серйозний вплив на економічну стабільність країни та впровадження прозорих та ефективних економічних політик.*

Аналітики виявляються ключовими учасниками цього процесу, оскільки вони застосовують передові методи аналізу великих обсягів фінансових даних, виявляють невідомі зв'язки та патерни, що допомагають не лише виявити злочинців, але й уникнути подібних порушень у майбутньому. Їхні високоспеціалізовані навички та здатність оперативно реагувати на зміни у фінансовому середовищі забезпечують ефективне функціонування системи розслідування, навіть в умовах що склались після повномасштабного вторгнення рф.

> *За спільними оцінками Міністерства економіки та Київської школи економіки станом на початок 2023 року загальні втрати України у війні склали близько 400 мільярдів доларів.*

Тому, з початку війни весь аналітичний сектор правоохоронних органів, починаючи від поліції і закінчуючи Службою безпеки України, зосередив свої зусилля задля виявлення російського бізнесу на території України [10].

> *Як результат станом на початок 2023 року було накладено арешти на рухоме і нерухоме майно підприємств РФ на загальну суму близько 38 млрд грн. [11].*

Враховуючи такі дані, важливу роль у роботі українських аналітиків щодо пошуку російських активів почала відіграла консолідована робота з міжнародними інституціями та участь у міжнародних проектах, адже до приховування російських капіталів та створення тіньових схем відмивання «брудних» коштів бізнесу держави-агресора були залучені команди досвідчених юристів-міжнародників, експертів у сфері економіки.

Водночас, в умовах війни та обмежених ресурсів, аналітична робота зосередилась на двох напрямах:

- *пошуку в Україні активів, які належать рф та її громадянам, які підтримують агресію;*
- *виявлення закордонних активів агресора: участь у зборі доказової бази задля подальшої конфіскації та передачі Україні.*

Завдяки цій роботі вдалося перевірити низку підсанкційних осіб країни-агресора, встановити їх активи на території України. Крім того,

> *з початку війни аналітики долучилися до проекту Офісу Генерального прокурора України «Task Force» - Міжвідомчої робочої групи з питань притягнення до відповідальності осіб, причетних до агресії проти України, розшуку, виявлення та арешту активів, а також об'єктів права власності рф та її резидентів.*

За результатами цієї міжнародної співпраці робочій групі вдалося заморозити значні активи росіян, навіть не зважаючи на прихований вплив російського капіталу на лобіювання інтересів російських політичних кіл в Україні через, так званих, агентів впливу, та відповідно поширення російських наративів.

Значна увага приділяється плануванню аналітичного дослідження. Така діяльність аналітика спрямована, в першу чергу, на визначення ключових індикаторів:

- *виявлення активів політично значущих осіб держави-агресора, які мають офіційно зареєстровані активи на власне ім'я на території України;*
- *встановлення підприємств, що мають зв'язки з військово-промисловим комплексом рф;*
- *на регіональному рівні – виявлення пов'язаних фірм – лідерів з отримання доходів за своїм основним видом діяльності;*
- *підтвердження приналежності виявлених активів до фігуранта розслідування.*

Після виконання цих кроків перед аналітиком постають виклики здійснення загальної оцінки необоротних та оборотних активів, прибутків та видатків, а також визначення кола осіб, які мають права на активи, в тому числі реальних та бенефіціарних власників, де в першу чергу, увага зосереджується на наявності фірм-прокладок та офшорних трастів.

> *Процес розвитку підрозділів кримінального аналізу не зупинився, а навпаки отримав додатковий імпульс, що з одного боку поставив службу перед фактом відсутності часу на роздуми, а з іншого – вплинув на креативність при реалізації нових проєктів.*

Це створює суттєве навантаження на кожного спеціаліста в цій галузі, але у свою чергу змушує брати на озброєння новітні технології на основі штучного інтелекту, хмарних обчислень та інших інновацій. А також особливу увагу звертати на розвиток людського потенціалу, підвищення ефективності роботи аналітиків відповідно до завдань, окреслених у Комплексному стратегічному плані реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки [12].

У розбудові потенціалу служби одним із основних пріоритетів Департаменту кримінального аналізу є активна взаємодія з міжнародними партнерськими організаціями такими як Консультативна місія Європейського Союзу (EUAM), Місія регіонального програмного офісу Міжнародної програми підвищення кваліфікації органів кримінального розслідування (ICITAP) в Україні та відділ з правоохоронних питань (INL) Посольства США в Україні. За цей час відбулося близько 30 онлайн та офлайн зустрічей, на яких обговорювалися перспективи розвитку служби на основі світових стандартів аналізу злочинності та загалом аналітичної розвідки.

Також, уперше з моменту створення служби працівниками підрозділів кримінального аналізу всіх рівнів разом з більш ніж 800 аналітиками з 25 країн взято участь у 33-тій щорічній навчальній конференції, організованій «Міжнародною асоціацією аналітиків злочинності» (IACA), що проходила у м. Даллас (штат Техас, США).

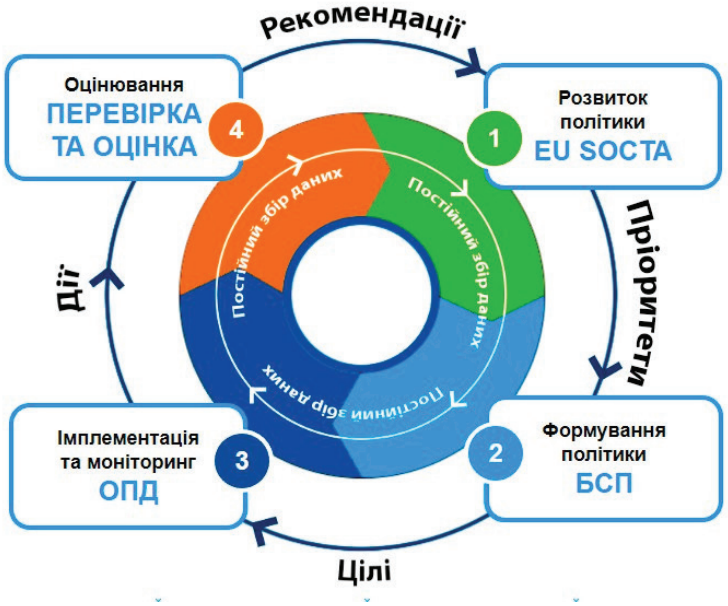
ІМПЛЕМЕНТАЦІЯ МЕТОДОЛОГІЇ SOCTA ТА СТАНДАРТІВ ЄС З ПРОТИДІЇ КРИМІНАЛЬНИМ ЗАГРОЗАМ

Організована злочинність загрожує миру та безпеці людей, ставить під загрозу реалізацію прав людини та підриває економічний, соціальний, культурний, політичний і громадянський розвиток суспільств у всьому світі [13]. Проте правоохоронні органи можуть розслідувати лише невеликий відсоток інформації та аналітичних даних, які вони здобувають щодо організованої злочинності та організованих злочинних мереж у своїх відповідних юрисдикціях. Тому оцінювання рівня цих загроз та визначення їх пріоритетності, а також розподіл наявних людських, фінансових і технічних ресурсів є життєво важливим [14].

Модель ILP забезпечує базис, що потребує сучасний підхід та впровадження організаційними структурами того, що зазвичай визнається єдиним життєздатним вибором ефективного впливу на транснаціональну організовану злочинність, а саме: аналіз даних та інформації, обмін ними та співпраця, усунення виявлених та оцінених загроз у пріоритетний та цілеспрямований спосіб.

> *Сучасна просунута аналітика даних може допомогти правоохоронним органам розставити пріоритети у своїх зусиллях та забезпечити по-справжньому розумну поліцейську діяльність, керовану аналітичною розвідкою. – Європол [15].*

У 2010 році ЄС розробив Цикл політики ЄС щодо серйозної та організованої злочинності (EU Policy Cycle for Serious and Organized Crime), який представлено як приклад передової практики щодо впливу на організовану злочинність відповідно до принципів ILP [16].



Цикл політики ЄС спрямовано на створення цілісної системи та ефективних оперативних дій щодо подолання найгостріших кримінальних загроз, що постають перед ЄС. Цикл політики створює можливість і націлює на інтеграцію між різними структурами в рамках мультидисциплінарного підходу, у тому числі для створення синергії між правоохоронними органами та відомствами охорони кордонів, сприяння

подальшій співпраці між європейськими установами, а також із зацікавленими сторонами, які не входять до ЄС.

Кожен цикл політики охоплює загалом чотири роки та складається з чотирьох основних кроків.

1 – оцінка загроз серйозних злочинів та організованої злочинності ЄС (SOCTA). SOCTA розроблена та оприлюднена Європолом у співпраці з Дорадчою групою SOCTA (у складі представників країн-членів ЄС, установ ЄС, Європейської комісії та Ради Генерального Секретаріату) за підтримки третіх країн-партнерів Європолу та організацій. Оскільки методологія схвалена Радою міністрів юстиції та внутрішніх справ ЄС, вона має чітку правову основу та потужну політичну підтримку[17].

Процес SOCTA Європолу включає [14]:
- *підготовка та узгодження деталізованих вимог замовника;*
- *підготовка та узгодження методології;*
- *визначення вимог до аналітики;*
- *збір даних;*
- *аналіз даних;*
- *підготовка звіту SOCTA, включаючи перелік ключових загроз і ризиків; і*
- *представлення результатів і рекомендованих пріоритетів.*

Процес аналізу здійснюється шляхом зосередження уваги на чотирьох елементах. Для кожного з них збираються конкретні дані [14]:
- *сфери/види серйозної та організованої злочинності;*
- *організовані злочинні групи/мережі та окремі суб'єкти, причетні до вчинення серйозних злочинів;*
- *середовище: вразливості, можливості та інфраструктура; і*
- *наслідки та шкода.*

Оцінювання загроз не є описовими звітами щодо поточного стану, а спрямовані на прогноз майбутнього. Вони містять висновки з переліком ключових загроз та рекомендаціями щодо їх пріоритетності [14]. Звіти Європолу SOCTA подаються до Постійного комітету ЄС з оперативного співробітництва у сфері внутрішньої безпеки (COSI), де вони обговорюються у рамках процесу формування політики ЄС. Таким чином, остаточне рішення є сукупністю професійних оцінок експертів і політичних поглядів.

2 – багаторічні стратегічні плани. На підставі SOCTA Рада міністрів юстиції та внутрішніх справ ЄС приймає офіційне рішення про пріоритетні сфери протидії злочинності на наступні чотири роки. Визначаючи політику, Рада враховує коментарі від країн-членів ЄС, установ та країн-партнерів, які не входять до складу ЄС.

За кожним із пріоритетів група експертів із найбільш уражених країн складає *багаторічний стратегічний план* (БСП), розрахований на чотири роки. Ці міждисциплінарні плани містять перелік стратегічних цілей, які мають бути досягнуті протягом чотирирічного циклу. У всіх планах визначено ключові індикатори ефективності, часові рамки, контрольні точки та відповідальні установи/особи [14]. БСП набувають формального статусу, під які виділяються фінансові ресурси.

3 – оперативні плани дій. Кожен БСП розгортається у річний *оперативний план дій* (ОПД) за відповідним пріоритетом. Усі ОПД описують кроки та дії інституцій та агенцій ЄС, а також дії, які виконуватимуться окремими національними органами.

Спільні дії в рамках ОПД реалізуються у рамках механізму Європейської мультидисциплінарної платформи протидії кримінальним загрозам (European Multidisciplinary Platform Against Criminal Threats - EMPACT) [14]. Цей механізм забезпечує структуровану платформу співпраці для відповідних держав-членів, інституцій та агенцій ЄС, а також залучених партнерів, які не є членами ЄС. Імплементацію кожного ОПД очолює орган з держави-члена ЄС, який добровільно виявив бажання виконувати цю роль, а на національному рівні контроль здійснюють національні координатори з питань EMPACT (НЕК), призначені у кожній країні-члені ЄС. Європол надає адміністративну та логістичну підтримку проектам EMPACT та контролює їх прогрес. Європол також призначає менеджерів служб підтримки EMPACT для забезпечення аналітичної та оперативної підтримки всіх пріоритетів щодо злочинності [14].

Всім національним органам ЄС пропонується і настійно рекомендується інтегрувати БСП та ОПД у свої національні процеси планування та зусилля правоохоронних органів щодо протидії серйозній та організованій злочинності. Відповідним агентствам ЄС також рекомендується визначати пріоритети та плани діяльності у своїх річних робочих програмах.

4 – огляд та оцінка. По завершенню терміну ОПД перевіряється їх ефективність та вплив на пріоритетні загрози. Щорічна звітність національних органів та проміжна оцінка з боку Європолу забезпечують можливість адаптації або зміни БСП, або пріоритетів у разі потреби. На основі щорічного звіту про стан справ, наприкінці кожного циклу реалізації політики, проводиться ретель-

на незалежна оцінка [14]. Уроки, отримані з цієї оцінки, є джерелом інформації для формування політики на наступний цикл.

SOCTA Україна

Україною вжито низку заходів з виконання взятих на себе зобов'язань перед ЄС у сфері протидії кримінальним загрозам, зокрема організованій злочинності. Так, у 2020 році Кабінетом Міністрів України схвалено Стратегію боротьби з організованою злочинністю, яка визначає напрями розвитку системи боротьби з організованою злочинністю та механізми реалізації державної політики у цій сфері в сучасних умовах [18].

Зокрема, Стратегією передбачено три етапи її реалізації. На першому етапі здійснюється оцінка загроз тяжких злочинів та організованої злочинності (SOCTA Україна). На другому етапі за результатами проведеної оцінки визначаються стратегічні цілі і розробляються комплексні плани заходів. Третій етап передбачає виконання зазначених вище комплексних планів заходів.

До завдань, які стоять перед SOCTA Україна, слід визначити такі:
- *проведення аналізу тенденцій організованої злочинності;*
- *здійснення аналізу сфер діяльності організованих груп і злочинних організацій (далі – ОГ і ЗО);*
- *узгодження цілей та завдань з протидії організованій злочинності;*
- *аналіз законодавства у сфері протидії організованій злочинності;*
- *оцінка ефективності здійснення заходів з протидії ОГ і ЗО;*
- *аналіз можливостей досягнення цілей та виконання завдань;*
- *інші заходи організаційного та аналітичного характеру;*

Реалізація проєкту за методологією Європейського поліцейського офісу SOCTA Україна здійснюється у 3 етапи:
1. *підготовчий (організаційно-методичний, первинний збір інформації);*
2. *обробка та внесення даних до ІП «SOCTA»;*
3. *аналіз та оцінка зібраних даних.*

На сьогодні завершено І (підготовчий) етап упровадження SOCTA Україна. До його результатів можна віднести те, що в січні 2022 року Кабінетом Міністрів України затверджено склад та Положення міжвідомчої робочої групи з координації запровадження в діяльність центральних органів виконавчої влади SOCTA Україна, *до якої зокрема входять представники МВС, Національної поліції, ДПС, СБУ, ДБР, ОГП, БЕБ, НАБУ, РНБО*. Крім того схвалено Порядок збирання і узагальнення інформації та здійснення оцінювання загроз організованої злочинності та тяжких злочинів відповідно до SOCTA Україна» [19].

Міністерством внутрішніх справ і Національною поліцією забезпечено функціонування вищезгаданої міжвідомчої робочої групи, на засіданнях якої визначено 4-річний період оцінювання загроз організованої злочинності за методологією SOCTA – 2019-2022 роки; затверджено, запропоновані Національною поліцією, типові форми облікових карток щодо організованої групи та/або злочинної організації, злочинної спільноти та щодо сфер злочинної діяльності [20].

У результаті проведених підрозділами кримінального аналізу звірок відомостей, отриманих з регіонів, та матеріалів щодо протидії організованій злочинності, наданих Офісом генерального прокурора України, визначено перелік кримінальних проваджень відносно ОГ і ЗО, які було направлено до суду в період з 2019 по 2022 роки, та які підлягають оцінці за методологією SOCTA.

Також відбулося затвердження запропонованого Національною поліцією переліку сфер злочинної діяльності, які будуть вивчатися у ході проведення оцінювання загроз організованої злочинності відповідно до методології SOCTA Україна, а також органів, відповідальних за заповнення відповідних облікових карток [21].

Крім того, у грудні 2022 року в структурі Департаменту кримінального аналізу створено 4-й відділ (оцінки загроз та стратегічного аналізу) 1-го управління (аналітичного), на який покладено завдання щодо проведення стратегічного кримінального аналізу, у т. ч. у межах проєкту SOCTA.

На даний момент триває 2-й етап реалізації проєкту, який передбачає обробку та внесення даних до інформаційної підсистеми «SOCTA». Зокрема, з метою автоматизації процесу збору даних про викриті ОГ і ЗО розроблено відповідне ІТ-рішення – Інформаційну підсистему ІПНП України «SOCTA». Слід зазначити, що в більшості країн ЄС дотепер працівники поліції збирають відомості в ручному форматі за допомогою таблиць програми Excel.

Інформаційна підсистема ІПНП України «SOCTA» - це спільний проєкт Департаменту кримінального аналізу та Департаменту інформаційно-аналітичної підтримки, який розпочав тестову експлуатацію із залученням працівників інших оперативних підрозділів Національної поліції на центральному рівні.

На виконання підпункту 2 пункту 4 протокольного рішення, ухваленого на засіданні Міжвідомчої робочої групи з координації запровадження в діяльність центральних органів виконавчої влади SOCTA Україна [22] та за дорученням Міністерства внутрішніх справ України розроблено проєкт наказу Міністерства внутрішніх справ України «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «SOCTA» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України».

У структурі ІП «SOCTA» передбачено 2 форми облікових карток (запитальників):

1. Облікова картка щодо організованої групи та/або злочинної організації, злочинної спільноти, яка заповнюється окремо на кожну організовану групу та/або злочинну організацію, злочинну спільноту.

2. Облікова картка щодо сфер злочинної діяльності, яка заповнюється окремо на кожну сферу злочинної діяльності, причому кожна сфера злочинної діяльності оцінюється за визначеним переліком індикаторів.

Зазначені картки створені у формі запитальників, що містять індикатори, які дозволяють цілісно зрозуміти та оцінити рівень організованої злочинності.

Методологія оцінювання використовує змішаний підхід, який складається з якісних та кількісних методів аналізу та набору чітко визначених показників для виявлення та уточнення найбільш загрозливих кримінальних явищ.

На підставі зібраних даних остаточно ухвалено перелік кримінальних проваджень відносно ОГ і ЗО, які було направлено до суду у період з 2019 по 2022 роки та які підлягають оцінці за методологією SOCTA. Також визначено перелік пріоритетних сфер злочинної діяльності.

До переліку пріоритетних сфер злочинної діяльності, які підлягають оцінці за методологією SOCTA, входять:

- *торгівля людьми*
- *нелегальна міграція*
- *незаконний обіг наркотичних засобів*
- *кіберзлочинність*
- *фальсифікація товарів (у галузі харчової промисловості, фармацевтична галузь, тощо)*
- *порушення авторського права і суміжних прав*
- *корупція*
- *легалізація (відмивання) доходів, одержаних злочинним шляхом*
- *зловживання (корупція) в спорті*
- *незаконна діяльність з організації або проведення азартних ігор, лотерей*
- *екологічна злочинність (незаконний обіг відходів, торгівля зникаючими видами, тощо)*
- *підроблення грошей, цінних паперів, білетів державної лотереї, марок акцизного податку чи голографічних захисних елементів*
- *незаконна діяльність з підакцизними товарами (алкоголь, тютюн, нафтопродукти, тощо)*
- *рейдерство*
- *підроблення документів*
- *вимагання (рекет, шантаж)*
- *незаконний обіг вогнепальної зброї*
- *викрадення людей*
- *вбивство*
- *встановлення або поширення злочинного впливу*
- *злочини проти власності (крадіжка, грабіж, розбій, привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем, тощо)*
- *незаконне заволодіння транспортними засобами, культурними цінностями та артефактами*
- *шахрайство*

Важливо зазначити, що якість кінцевого аналітичного продукту залежить від якості внесених у підсистему даних. З метою оптимізації процесу внесення даних та контролю за їх якістю в центральному органі управління поліцією та Головних управліннях Національної поліції в областях та м. Києві створено робочі групи, на які покладено цей обов'язок. До складу таких робочих груп включені співробітники слідчих, оперативних та аналітичних підрозділів.

Основними вимогами до членів робочої групи є те, що співробітники, які включені до робочих груп, повинні мати достатній рівень знань про криміногенну ситуацію в регіоні, особливості розслідування та документування кримінальних правопорушень, учинених організованими групами та злочинними організаціями, а також мати навички роботи з великими обсягами інформації, складання аналітичних документів.

З метою забезпечення повного та своєчасного внесення даних до облікових карток ІП «SOCTA» працівниками Департаменту кримінального аналізу підготовлено відповідний методичний посібник, постійно проводилась роз'яснювальна робота по внесенню інформації, проведено ряд занять з членами робочих груп, детально роз'яснено обсяг інформації, необхідний для внесення по кожному з індикаторів, а також зазначено джерела отримання такої інформації.

Після внесення даних до ІП «SOCTA» буде проведено 3-й етап проєкту – опрацювання отриманої інформації, її аналіз та підготовлено відповідний аналітичний звіт, який готуватиме міжвідомча аналітична група.

Звіт буде включати аналітичні висновки, що сформують політичні пріоритети, які трансформуються в стратегічні правоохоронні цілі. Затверджені стратегічні цілі стануть основою для розроблення комплексних планів заходів.

На четвертому засіданні Міжвідомчої робочої групи з координації запровадження в діяльності центральних органів виконавчої влади системи оцінки SOCTA Україна, затверджено методологію оцінювання загроз серйозної та/або організованої злочинності в Україні (SOCTA Україна), яка розроблена Міжвідомчим науково-дослідним центром з проблем боротьби з організованою злочинністю.

ВИКОРИСТАНІ ДЖЕРЕЛА:

1. Наказ Національної поліції України від 08 квіт. 2016 р. № 296 дск.
2. Про введення воєнного стану в Україні: Указ Президента України від 24 лют. 2022 р. № 64/2022. URL: https://www.president.gov.ua/documents/642022-41397.
3. Наказ Національної поліції України від 22 черв. 2022 р. № 439.
4. Наказ Національної поліції України від 13 грудня 2022 р. № 886.
5. Наказ Національної поліції України від 27 квіт. 2023 р. № 340.
6. Методичні рекомендації щодо організації та проведення кримінального аналізу підрозділами Національної поліції України (від 26 травня 2021 року № 6516/01/33-2021).
7. Наказ Національної поліції України від 19 жовт. 2023 р. № 952.
8. Кримінальний кодекс України: Закон України від 05 квіт. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.
9. Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: https://zakon.rada.gov.ua/laws/show/984_008-16
10. Звіт про прямі збитки інфраструктури та непрямі втрати економіки від руйнувань внаслідок військової агресії Росії проти України станом на червень 2023 року. URL: https://damaged.in.ua/damage-assessment.
11. Звіт Національної поліції України про результати роботи у 2022 році. URL: https://www.kmu.gov.ua/news/zvit-natsionalnoi-politsii-ukrainy-pro-rezultaty-roboty-u-2022-rotsi\.
12. Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки: Указ Президента України від 11 трав. 2023 р. № 273/2023. URL: https://zakon.rada.gov.ua/laws/show/273/2023#Text
13. United Nations. Office on Drugs and Crime. URL: www.unodc.org/unodc/en/organized-crime/index.html?ref=menuside
14. *OSCE Guidebook Intelligence-Led Policing* (2017). TNTD/SPMU Publication. Series Vol. 13. Vienna.
15. Europol, Exploring Tomorrow's Organized Crime.The Hague: European Police Office, 2015. URL: https://www.europol.europa.eu/publications-documents/exploring-tomorrow's-organised- crime
16. Council conclusions on the creation and implementation of a EU policy cycle for organized and serious international crime: 3043rd Justice and Home Affairs Council Meeting. (Brussels: 8 and 9 November 2010). URL: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/117583.pdf
17. Serious and Organised Crime Threat Assessment 2017 – Revised methodology. Council of the European Union. Doc. 14913/15, CRIMORG 128 (Brussels: 11 December 2015).
18. Про схвалення Стратегії боротьби з організованою злочинністю: Розпорядження Кабінету Міністрів України від 16 верес. 2020 р. № 1126-р. URL: https://zakon.rada.gov.ua/laws/show/1126-2020-%D1%80#Text
19. Деякі питання запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна: Постанова Кабінету Міністрів України від 26 січ. 2022 р. № 59. URL: https://zakon.rada.gov.ua/laws/show/59-2022-%D0%BF#Text
20. Протокол № 1 засідання Міжвідомчої робочої групи з координації запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна від 02 листоп. 2022 р.
21. Протокол № 2 засідання Міжвідомчої робочої групи з координації запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна від 11 січ. 2023 р.
22. Протокол № 3 засідання Міжвідомчої робочої групи з координації запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна від 23 черв. 2023 р.

DOI: https://doi.org/10.36486/978-966-2310-66-5-16

Хоч би які великі були московські насильства, вони не дають москалям жодного законного права на Україну

Пилип Орлик

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

Денис Пефтієв
Карен Ісмайлов

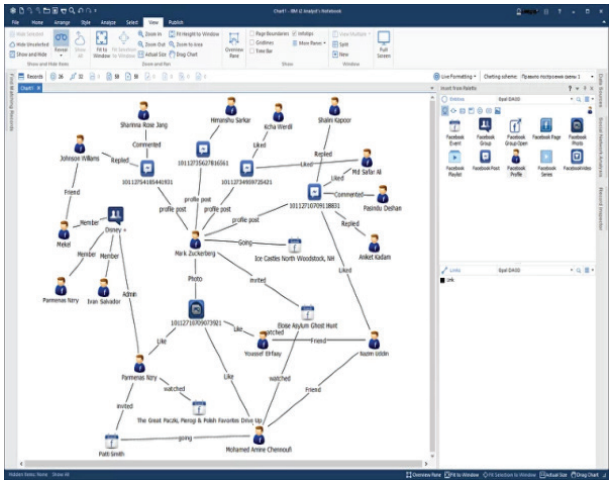
ІНСТРУМЕНТИ З ОБРОБКИ І АНАЛІЗУ ВЕЛИКОГО ОБСЯГУ ДАНИХ

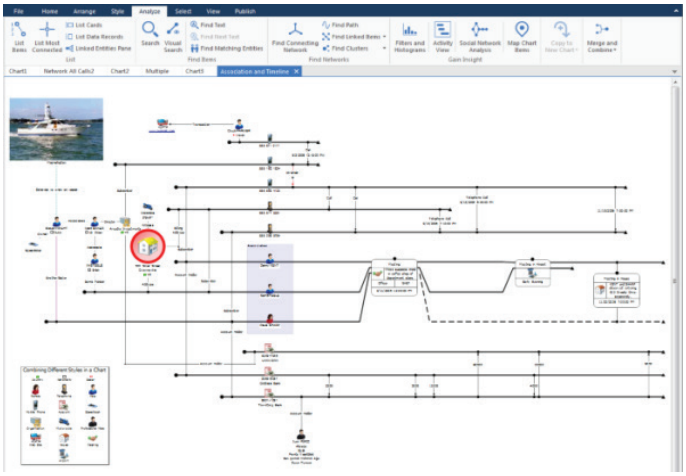
Обробка великої кількості інформації в OSINT може бути викликом через обсяг даних, які потрібно аналізувати. Щоб ефективно обробляти великі обсяги інформації в рамках OSINT, були створені інструменти, які можуть сприяти цьому процесу. Вони можуть значно полегшити процес обробки великої кількості інформації та дозволити здійснювати більш ефективний та точний аналіз даних.

Також, вони надають можливості для створення комплексних звітів та аналітичних висновків, що допомагає аналізувати інформацію з різних кутів та отримувати більше контексту для прийняття важливих рішень.

i2 Analyst's Notebook - надає розширені можливості аналізу зображень, які можуть допомогти швидко перетворити різноманітні набори складної інформації на дієву та високоякісну розвідку. Це допомагає аналітикам та іншим фахівцям, які займаються кримінальним аналізом, виявляти, прогнозувати й уникати злочинної, терористичної та шахрайської діяльності.

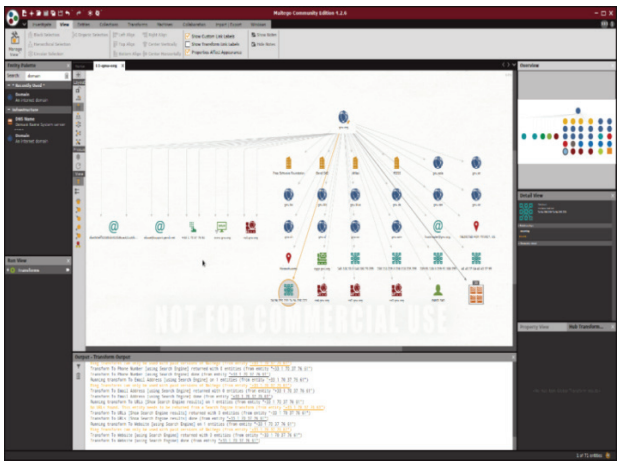
Крім того, у ньому гнучка модель даних і широкий спектр засобів візуального аналізу, призначених для того, щоб допомогти користувачам виявити ключові особистості, зв`язки, стосунки і відносини. Можуть бути упущені події, шаблони і тенденції. Крім того, він включає функції Social Network Analytics, призначені для глибшого розуміння соціальних відносин і структур у мережах, що становлять інтерес.





Maltego - потужне програмне забезпечення по збору інформації (OSINT) з відкритим вихідним кодом. Програма дозволяє шукати інформацію в профілях соціальних мереж, за адресами електронної пошти, за номерами телефонів і не тільки.

Така інформація буде доступна будь-якій людині чи компанії для вирішення професійних питань. За допомогою Maltego можна визначити геолокацію

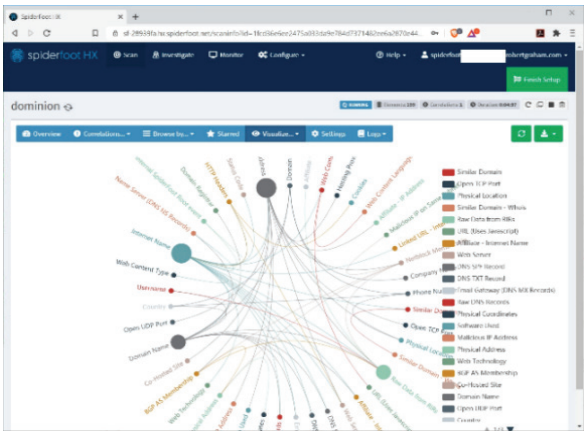


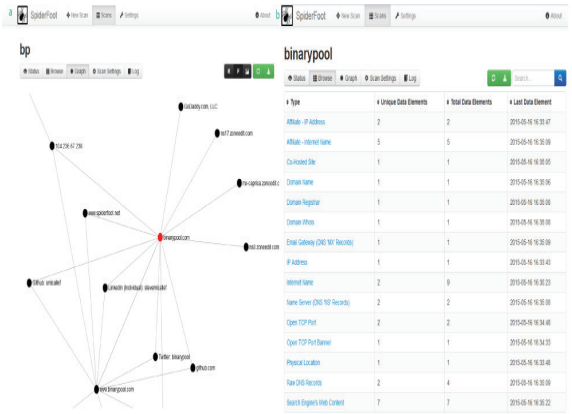
кіберзлочинців, дізнатися особисті дані. У судових розслідуваннях, криміналістиці це ПЗ стане чудовим помічником. Шахраї можуть використовувати різні схеми обману – атакувати спамом, реєструвати фішингові домени, зламувати облікові записи та ін. Програма Maltego здатна виявляти злочинців. Часто програмне забезпечення допомагає журналістам шукати потрібну інформацію, наприклад під час розслідування. Програма є корисною для правоохоронних органів, приватних детективів. Цей Java-додаток аналізує посилання у графічному вигляді, працює на всіх операційних системах (Windows, Mac, Linux).

Аналіз здійснюється за допомогою запиту записів DNS, whois, пошукових систем, різноманітних API, отриманням метаданих. Результати представлені у вигляді графічних макетів. Таким чином є можливість групувати дані для візуального відображення взаємозв`язків.

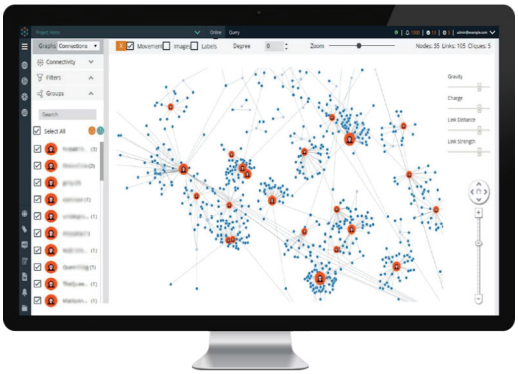
SpiderFoot - інструмент для збору інформації з відкритих джерел (OSINT). Утиліта, призначена для автоматизації пошуку інформації про ціль (представленої IP-адресою, доменним ім'ям та електронною поштою тощо). Поряд із платною версією, розробники пропонують і безкоштовну версію SpiderFoot з відкритим вихідним кодом.

За допомогою SpiderFoot можна автоматизувати процес пошуку і збору інформації про задану мету. У документації до інструменту пояснюється, що SpiderFoot може збирати такі відомості, як Whois, веб-сторінки, DNS і багато іншого. На відміну від свого аналога Maltego, інтерфейс SpiderFoot доступний у браузері.





COBWEBS (Tangles та Weblock) - модуль програмного забезпечення Tangles дозволяє здійснювати пошук за ідентифікаторами, такими як номер телефону, ім'я, нікнейм в соціальних мережах та месенджерах, дозволяє здійснювати пошук постів у соціальних мережах за ключовими словами та хештегами, існує можливість здійснення поглибленого аналізу кожного акаунту, що привернув увагу, а саме: проведення додаткових досліджень на основі постів, списку друзів, приналежності до груп тощо, існує можливість здійснювати пошук по зображенням, а також шукати визначений текст на зображеннях, дозволяє відображати регіони на карті, у разі згадування в постах конкретного регіону, або якщо фото/відео пов'язане з конкретною локацією, дозволяє здійснювати моніторинг трендів у заданій локації з визначеним радіусом (працює в X (в минулому Twitter)).



Weblock Cobwebs надає реальну інформацію про місця, людей і дані, що становлять інтерес для різних організацій. Унікальні можливості розширюють можливості автоматичного аналізу інформації про місцезнаходження, а також дозволяють створювати і поширювати розвідувальні та слідчі звіти.

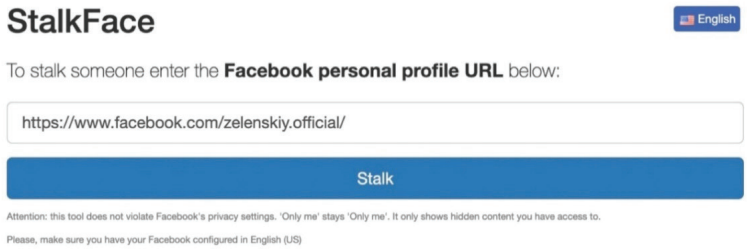
Продукт призначений для ретельного сканування нескінченних цифрових каналів з веб-екосистеми, збираючи та аналізуючи величезні обсяги даних про місцезнаходження, щоб допомогти вам захистити цінні активи. Платформа дозволяє здійснювати пошук та аналіз рекламних ідентифікаторів мобільних пристроїв Android Advertiser Identification (AAID) та Identifier for Advertiser (IDFA), що використовуються на платформах Android та iOS відповідно. Даний функціонал дозволяє відстежувати переміщення конкретного пристрою та робити аналітичні висновки на основі отриманих даних.

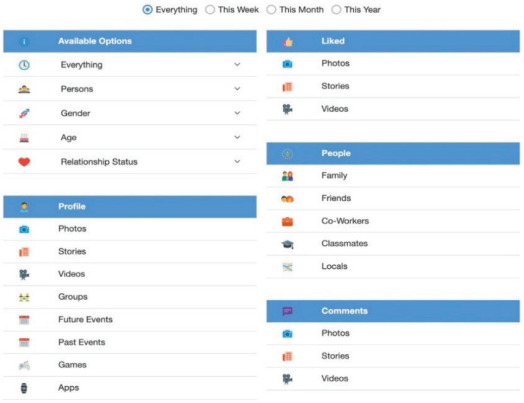


ПОШУК ОПЕРАТИВНО ЗНАЧУЩОЇ ІНФОРМАЦІЇ У ПОПУЛЯРНИХ СОЦІАЛЬНИХ МЕРЕЖАХ

Пошук інформації у соціальній мережі Facebook сервісом **StalkFace** (у минулому Stalkscan) – це сервіс, який дозволяє переглядати загальнодоступну інформацію про будь-якого користувача соціальної мережі Facebook. Для отримання інформації необхідно з цільової сторінки знайти профіль з відкритим доступом та ввести до поля посилання на сторінку та натиснути сканувати. Після цього необхідно вибрати потрібну інформацію в розділі. При виборі категорії користувач перенаправляється на сторінку соціальної мережі.

Також, окрім здобуття інформації за допомогою пошуку, *існує ще один вид пошуку за допомогою конкретизації посилань*.





Загальний пошук «Усі»	
Пошук серед дописів «Дописи». Серед дописів доступне наступне фільтрування:	- Вибір особи, яка публікувала допис «ДОПИСИ ВІД» - Вибір групи у якій опубліковано допис «ОПУБЛІКОВАНО В ГРУПІ» - Вибір місця що позначене у дописі «ПОЗНАЧЕНЕ МІСЦЕ» - Вибір коли публіковано допис «ДАТА ПУБЛІКУВАННЯ»
Пошук серед людей «Люди»	
Пошук у зображеннях «Світлини»	До пошуку серед світлин додано Фільтр «АВТОР»
Пошук серед відео файлів «Відео»	До пошуку серед світлин додано Фільтр «ДЖЕРЕЛО»
Пошук серед сторінок «Сторінки» Серед сторінок здійснюється фільтрування за категоріями:	- Будь-яка категорія - Місцевий бізнес чи місце - Компанія, організація чи установа - Бренд чи товар - Виконавець, гурт чи знаменитість - Розваги - Ініціатива чи спільнот
Пошук за місцями «Місце»	
Пошук у спільнотах «Групи»	
Пошук серед додатків «Додатки»	
Пошук серед подій «Події»	

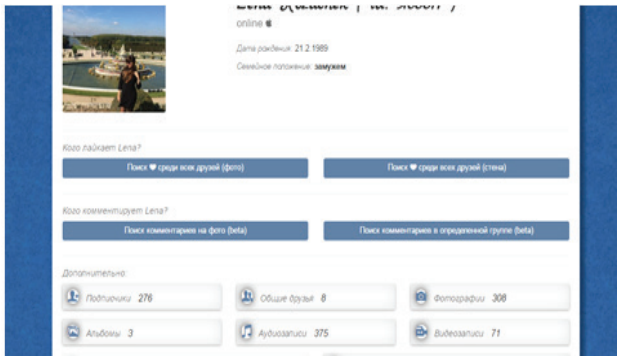
Всі ці дані на сервіси викладені в публічний доступ самими користувачами і беруться сервісом за допомогою офіційного API, тому не є персональними даними особи.

Ресурс **VK.WATCH** представляє собою інструмент для пошуку інформації про людей в соціальній мережі ВКонтакте та містить найбільший архів історичних даних сервісу VK: коментарі користувачів, фотографії, списки друзів та зміни профілів. Користувача можна знайти за унікальним ID або за останнім нікнеймом.



Ресурс **searchlikes.ru** допомагає в аналізі аккаунтів осіб в соціальній мережі ВКонтакте щодо їх дій, а саме:

- пошук лайків серед всіх друзів (фото);
- пошук лайків серед всіх друзів (стіна);
- пошук коментарів на фото;
- пошук коментарів в певній групі.



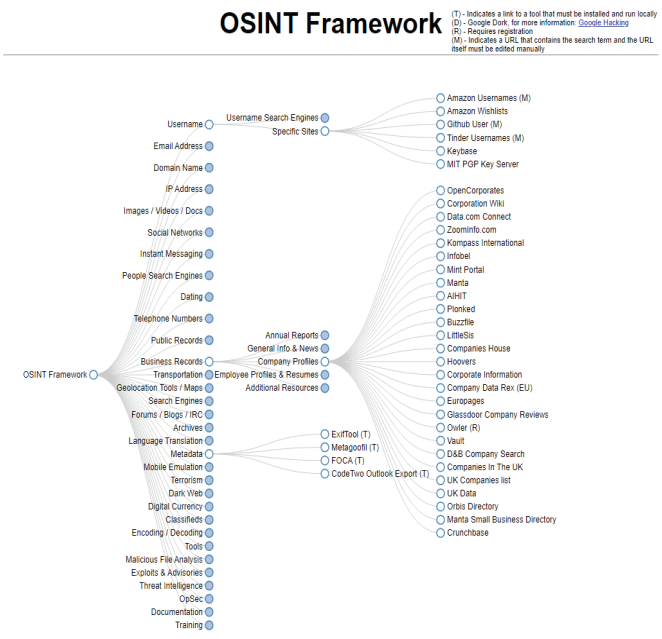
Osintgram – це інструмент OSINT в Instagram, який пропонує інтерактивну оболонку для виконання аналізу облікового запису Instagram будь-якого користувача за його псевдонімом.

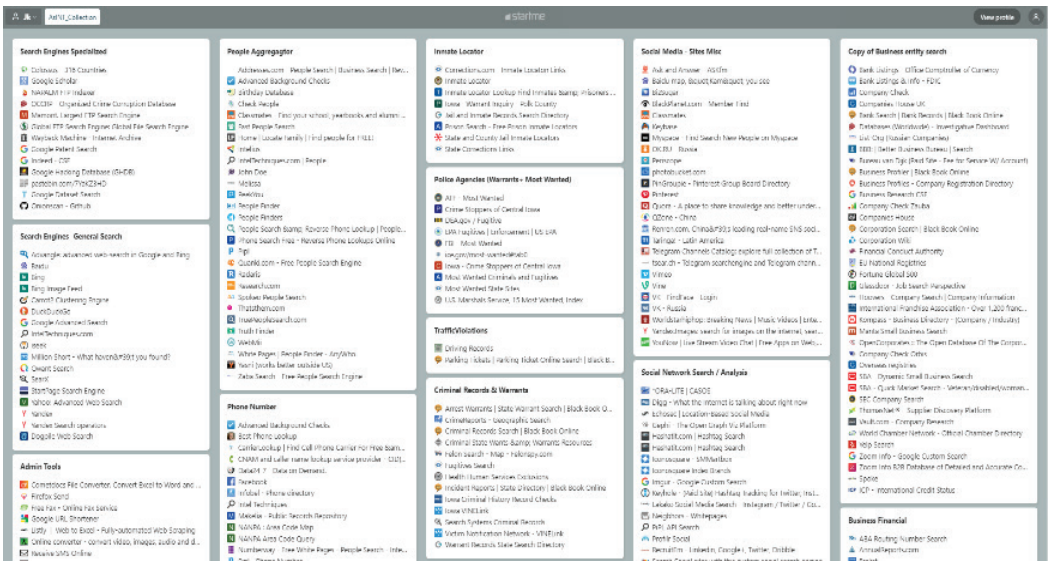
ФРЕЙМВОРКИ OSINT-ІНСТРУМЕНТІВ

Фреймворки OSINT-інструментів включають набір інструментів та методів, які використовуються для збору, аналізу та обробки відкритих джерел інформації. Ці фреймворки допомагають упорядковувати процес розвідки та досліджень, спрощуючи інтеграцію різноманітних інструментів та джерел даних.

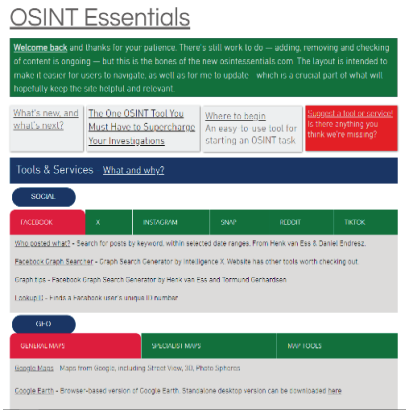
OSINT Framework - найбільший фреймворк OSINT інструментів, максимально простий та зручний інтерфейс. Всі інструменти структуровані на підрозділи, відповідно до їхнього призначення.

OSINT Framework орієнтований на збір інформації з безкоштовних інструментів або ресурсів. Мета - допомогти людям знайти безкоштовні OSINT-ресурси. Деякі з включених сайтів можуть вимагати реєстрації або пропонувати більше даних за підписку, але ви повинні мати можливість отримати принаймні частину доступної інформації безкоштовно.

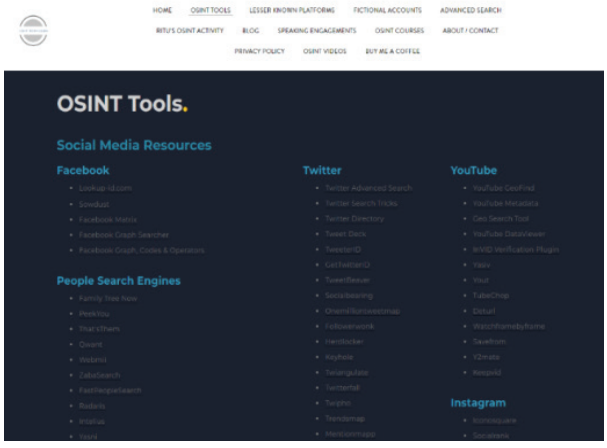




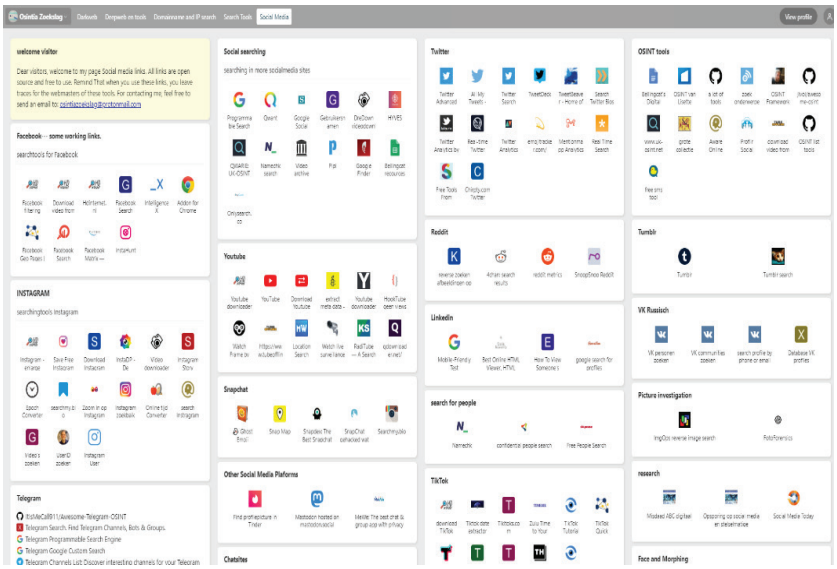
AsINT Collection – створений на базі порталу start.me репозитарій OSINT інструментів. Всі інструменти систематизовані, та охоплюють величезну кількість джерел інформації.



OSINT Essentials – сторінка надає посилання на здебільшого безкоштовні інструменти та служби, корисні для онлайн-перевірки, цифрової журналістики та розвідувальної роботи з відкритим кодом.



OSINT Tools - Колекція та набір інструментів, які використовуються для збору, аналізу та використання відкритої інформації з різних джерел



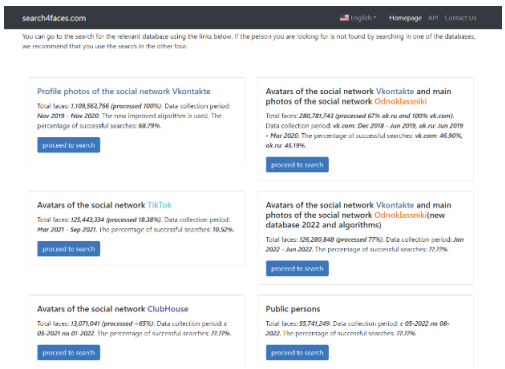
Social media – створений на базі порталу start.me репозитарій OSINT інструментів для роботи із соціальними мережами та іншими соціальними веб-продуктами.

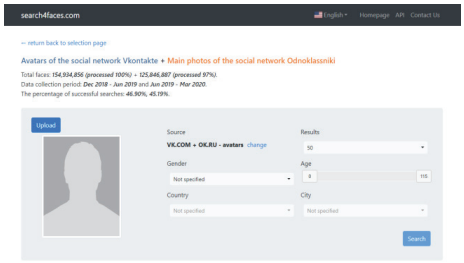
Всі інструменти систематизовані, та охоплюють величезну кількість джерел інформації.

АНАЛІТИЧНІ ПРОДУКТИ З АНАЛІЗУ ФОТО-ТА ВІДЕОМАТЕРІАЛІВ, А ТАКОЖ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ

При аналізі фото- та відеоматеріалів, а також розпізнаванні обличчя для OSINT (відкрите джерело розвідки) важливо використовувати ефективні інструменти, які дозволяють отримати важливу інформацію з відкритих джерел. Разом із розвитком штучного інтелекту, з'являються і інструменти по розпізнаванню обличчя, які допомагають в аналітиці.

search4faces - сервіс пошуку людей в інтернеті за фотографією. Завдяки технології нейронних мереж і машинному навчанню сервіс допоможе вам знайти потрібну людину або дуже на неї схожу протягом кількох секунд. Результатом є посилання на зображення в мережі або посилання на профіль знайденої людини в соціальній мережі vk.com або ok.ru, tiktok.com, clubhouse.com (а в найближчому майбутньому й інших).

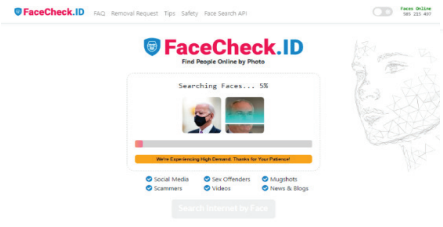


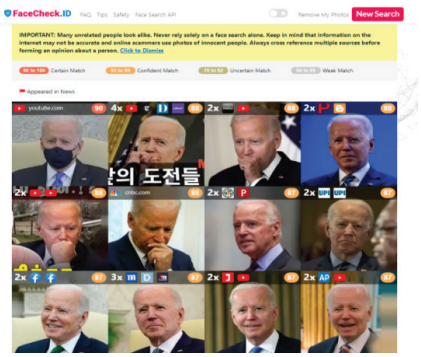


На поточний момент частково або повністю зібрано 5 баз даних: аватарки соціальної мережі Вконтакте і головні фотографії соціальної мережі Однокласники, фотографії профілю соціальної мережі Вконтакте, аватарки користувачів Tiktok, аватарки користувачів ClubHouse, база даних знаменитостей (Вікіпедія, ІМДБ та інші).

FaceCheck - це безкоштовний ресурс котрий дозволяє по одному лише фото провести пошук інформації від найвідоміших соцмереж до новини та навіть відео. За допомогою даного сервісу ви можете порівняти фотографію людини з мільйонами обличь з фотографій, які з'являлися в новинах.



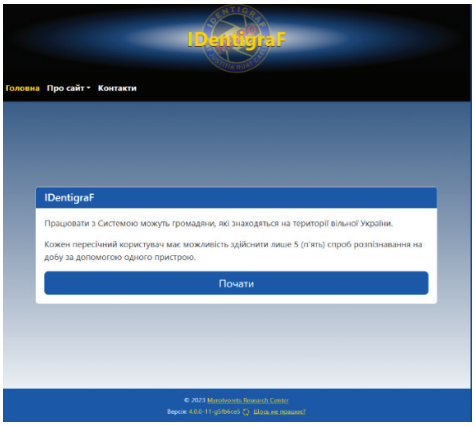




Також FaceCheck докладає всіх зусиль, щоб знайти та проіндексувати обличчя злочинців, ґвалтівників дітей, сексуальних злочинців, викрадачів, насильників, вбивць, злочинців на ґрунті ненависті, грабіжників, членів банд, втікачів, терористів, шахраїв на сайтах знайомств, аферистів та інших шахраїв.

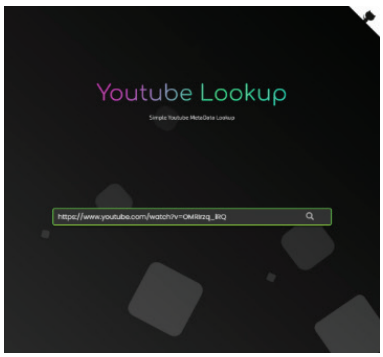
Водночас публічні особи також можуть бути об'єктом пошуку та добору фото особи.

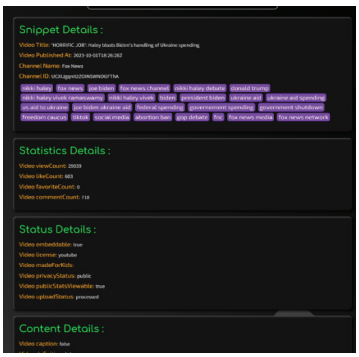
Система розпізнавання обличь «NEUROIDENTIGRAF» - розвинута система розпізнавання обличь, створена на основі нейромережі. Дана система може як і знайти особу в «Чистилищі», так і порівняти 2 фото. Кожен пересічний користувач має можливість здійснити лише 5 спроб розпізнавання на добу за допомогою одного мобільного пристрою.



Використання системи правоохоронними органами та силовими структурами України, спецслужбами країн – членів NATO та країн-партнерів, здійснюється на інших умовах, які не підлягають розголошенню.

Youtube Lookup - відображає метадані з відео, завантаженого на youtube. Також є можливість завантажити код із платформи github.





БАЗИ ДАНИХ У ВІДКРИТИХ ДЖЕРЕЛАХ

Бази даних у відкритих джерелах можуть включати різноманітні джерела даних, які доступні публічно та можуть бути використані для збору і аналізу інформації. Ці бази даних надають важливі відомості для досліджень, розвідки та аналізу в різних галузях. Деякі з популярних баз даних у відкритих джерелах включають:

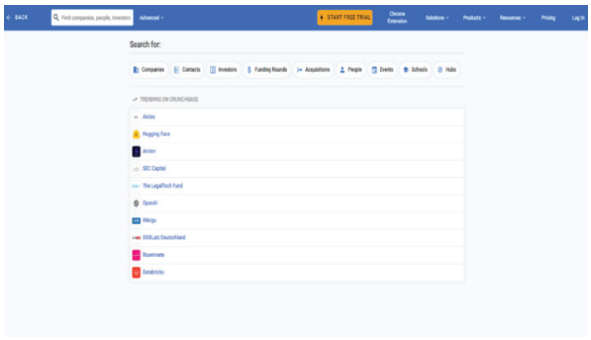
Державні бази даних: Це включає офіційні бази даних державних органів, такі як реєстри компаній, бази даних злочинів, даних про нерухомість, публічні фінансові звіти та багато іншого.

Соціальні медіа: Інформація з публічних профілів соціальних мереж, таких як Facebook, Twitter, LinkedIn та інших, може бути використана для отримання даних про людей, організації, події та багато іншого.

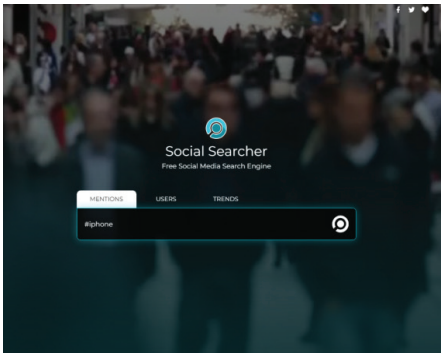
Новинні та медійні джерела: Інформація з новин, статей, прес-релізів та інших медійних джерел може бути використана для аналізу поточних подій та тенденцій.

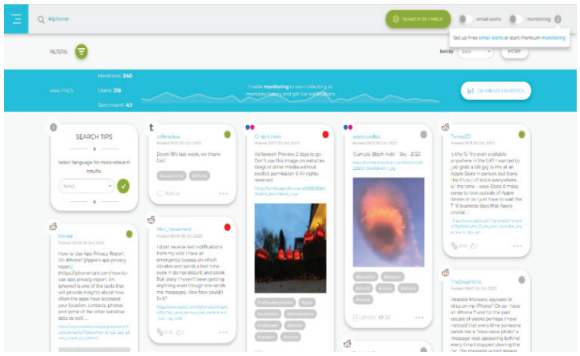
Відкриті бази даних дослідників та активістів: Це може включати бази даних, створені громадськими організаціями, дослідниками, журналістами та іншими, які надають важливі відомості про різні сфери діяльності.

Ці бази даних у відкритих джерелах надають важливий контекст та інформацію для аналізу даних у різних сферах, таких як дослідження, розвідка, розслідування та інші.



Crunchbase - це умовно безкоштовний інструмент котрий дозволяє шукати інформацію по назві компанії по всій земній кулі. Він надає доволі обширні результати від місця розташування до новин які пов'язані з цією компанією. Також надає доступ до особистої інформації і складу працівник, але це вже у платній версії. Головне що більшу частину інформації він видає безкоштовно, і в зручному для розумні вигляді.

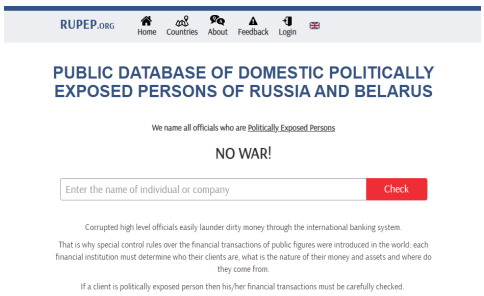




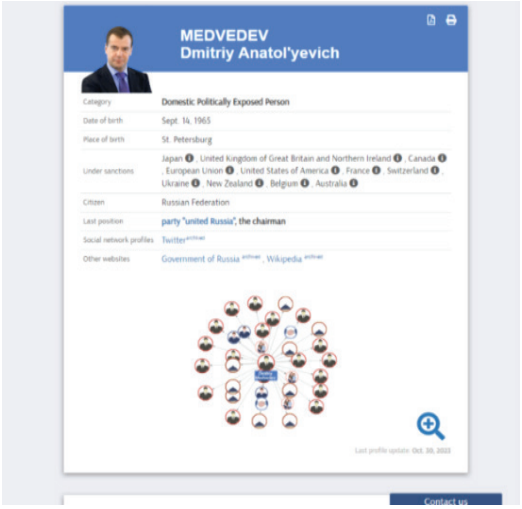
Social-Searcher - інструмент для пошуку профілів по прізвищу/імені або нікнейму в соцмережах.

Також дозволяє в реальному часі здійснювати пошук по ключовим словам та хештегам серед постів в Twitter, Google+, Facebook, Youtube, Instagram, Tumblr, Reddit, Flickr, Dailymotion та Vimeo. Існує можливість ставити пошук на моніторинг та додавати оповіщення на електронну пошту (в платних підписках). На сьогоднішній день також доступний додаток на платформі iOS.

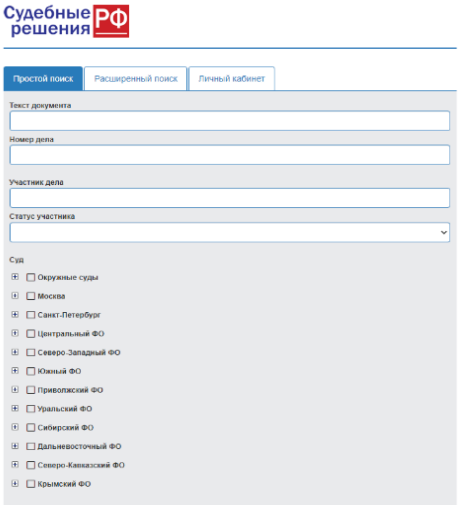
Відкрита база даних публічних посадових осіб росії та білорусі – на цьому сайті використано інформацію, отриману в рамках реалізації права вільно шукати, одержувати, передавати, виробляти і поширювати інформацію будь-яким законним способом.



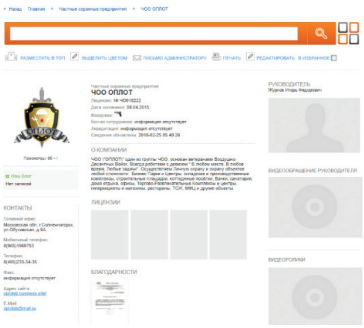
Використовуючи цей ресурс, можна визначити зв'язки осіб, їх кар'єрний шлях, декларації та багато чого іншого.



Пошук рішень судів загальної юрисдикції рф - спеціалізований інформаційний ресурс для публікації інформації про справи, що розглядаються судами загальної юрисдикції, і винесені ними рішення. Завдяки «Простому пошуку» користувачі можуть знайти справу за її номером, регіоном, судом, що ухвалив рішення, прізвищем судді, учасником, а також категорією. Форма «Розширеного пошуку» дає змогу шукати справи певної категорії, за номером статті Кримінального кодексу рф або Кодексу рф про адміністративні правопорушення, вибрати їх за датою ухвалення або надходження, а також відфільтрувати вибірку за результатами розгляду. Також можливий пошук за ПІБ.

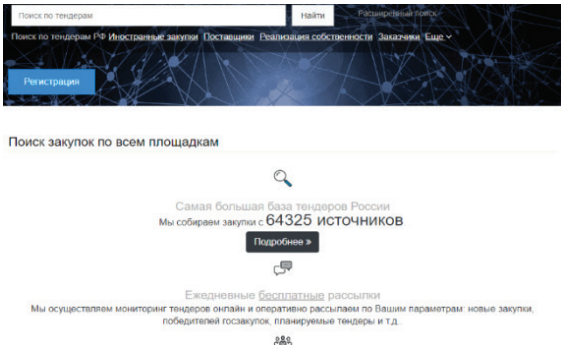


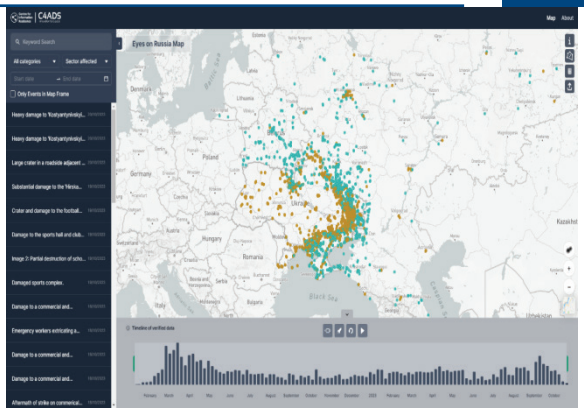
Інформаційно-аналітичний портал Allchop.ru - це універсальний інструмент, що позиціонується як інструмент для фахівців у сфері інформаційного забезпечення на ринку приватних охоронних послуг, що охоплює як сферу індустрії технічних засобів охорони, так і сферу послуг, що надаються охоронними підприємствами на території росії. Так як відомо, що в росії поширено реєструвати ПВК в якості охоронних фірм, даний ресурс допоможе знайти інформацію яка становить інтерес





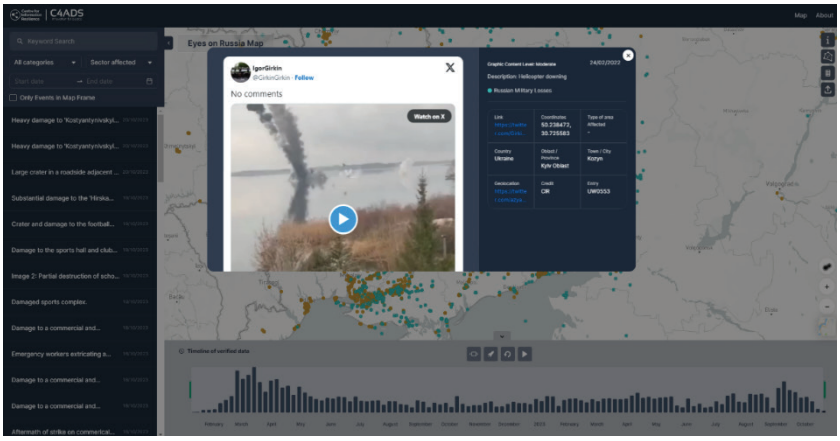
Тендерний портал TenderGuru.ru – агрегатор тендерів рф, а також країн СНГ. За допомогою даного сервісу можливо знаходити фінансові зв'язки між компаніями. Сайт має зручну навігацію та постійно актуальну інформацію. Є можливість настроювати розсилку по заданим параметрам і періоду збору інформації.



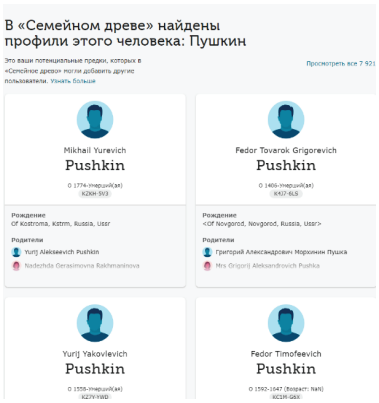


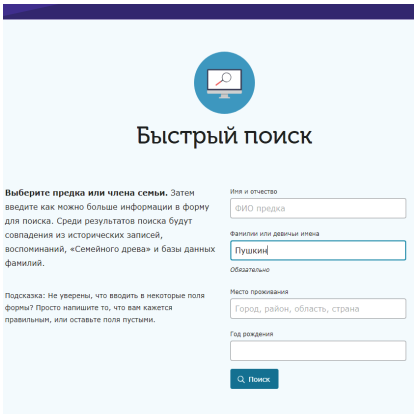
Eyes on Russia Map – проєкт для збору та перевірки відео, фотографій, супутникових знімків та інших медіа, пов`язаних з російським вторгненням в Україну. Мета проєкту проста: надати світові своєчасну та достовірну інформацію про вплив російського вторгнення на Україну та її народ.

Координуючи колективну роботу широкої спільноти відкритих джерел, включаючи Bellingcat і GeoConfirmed, за підтримки Advance Democracy, Inc. проект створив базу даних перевіреної інформації, що висвітлює події російського вторгнення. Карта «Eyes on Russia» була створена для того, щоб полегшити доступ громадськості до цієї інформації та її розуміння. Розроблена у співпраці з C4ADS, карта спирається на базу даних відео, фотографій, супутникових знімків та інших джерел, зібраних і перевірених проектом.



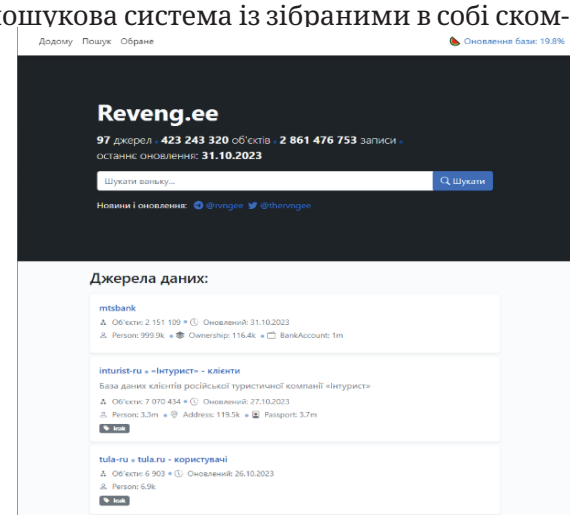
FamilySearch – веб-сайт із зібраною базою даних сімейних дерев, історичних записів та родоводів. Можна проводити пошук конкретного древа. Після введення прізвища сім`ї або назву місця, що відноситься до сім`ї, і сайт проведе пошук у своїх колекціях.





Також є можливість провести пошук суспільного дерева. Суспільне дерево – це колекція пов`язаних спорідненістю та підкріплених джерелами родоводів, що належать до певних періодів часу та спільнот. Вони створюються шляхом об`єднання компільованих та оригінальних джерел записів для побудови та вивчення родоводу спільноти. Ці записи включають дані з конкретних джерел, більшість з яких являють собою частини розширених родоводів і сімейних груп. Крім цього, є ще і інші можливості пошуку.

Reveng.ee – відкрита безкоштовна пошукова система із зібраними в собі скомпрометованих та «злитих» баз даних користувачів, клієнтів та іншої інформації російських компаній та сервісів.

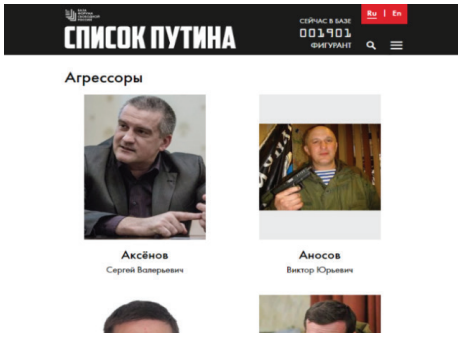


Станом на 31.10.2023 пошукова система має в своїй базі данних: 97 джерел, 423 243 320 об`єктів, 2 861 476 753 записи. Крім цього, оновлення бази данних відбувається часто, і під час цього сервіс продовжує свою роботу.

Є можливість пошуку по конкретним «злитим» базам, зберігати інформацію в «Обране» а також виставляти фільтри для пошуку інформації.

База «СПИСОК ПУТИНА» - база, створена Форумом вільної Росії з метою пошуку, закріплення та уніфікації даних про осіб, відповідальних за створення і функціонування системи узурпації влади і придушення громадянських свобод у Росії, а також військових злочинців та осіб, відповідальних за розпалювання війни.





База Форуму вільної Росії «СПИСОК ПУТИНА» працює на волонтерській основі і використовує інформацію з відкритих та інших джерел. База висловлює зацікавленість у співпраці з подібними проектами в Росії і за кордоном, і закликає до об`єднання і взаємного використання інформації для реалізації заявлених цілей.

Проєкт бачить своїм завданням збір інформації щодо осіб таких категорій:

«Власників» Росії, які захопили і злочинно утримують владу в країні;

«Виконавців», які безпосередньо реалізують як чиновники і депутати політику керівництва Росії зі злочинного утримання влади в країні;

«Правопорушників» з числа суддів, прокурорів, слідчих, адвокатів, співробітників оперативних служб та їхніх агентів, відповідальних за безпосереднє здійснення репресій і переслідування опозиції, представників громадянського суспільства та інших незгодних за політичними мотивами;

«Агресорів», відповідальних за проведення політики війни, окупації та хаосу щодо інших країн, порушення норм міжнародного права та міжнародних договорів у політичних інтересах керівництва РФ;

«Вигодоодержувач» - іноземних партнерів російської влади, які сприяють здійсненню її злочинних планів із руйнування принципів міжнародного права та міжнародної політики миру, демократії та протидії корупції.

«Олігархів і корупціонерів», відповідальних за розграбування Росії в державних масштабах, завдяки безпосередній участі у владі РФ або близькості до неї, зокрема, їхніх родичів і довірених осіб, причетних до відмивання здобутих у такий спосіб капіталів;

«Пропагандистів», відповідальних за створення і розповсюдження державної інформації, що навмисно спотворює і обманює людей, в інтересах політичного керівництва РФ, і насаджує в громадській думці агресію, атмосферу ненависті і політичну нетерпимість;

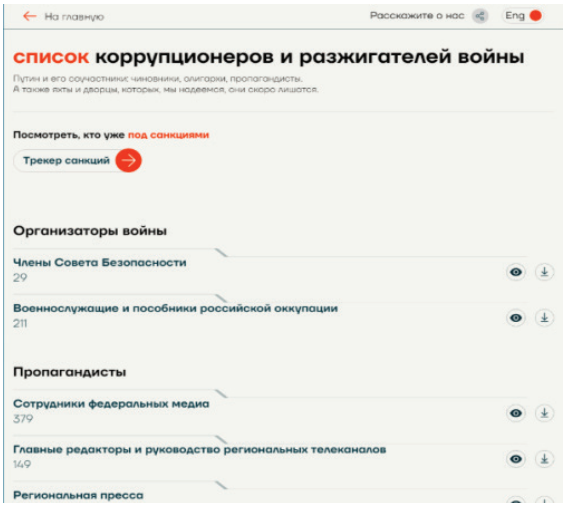
«Посібників» причетних до отримання злочинної та аморальної вигоди від співпраці з владою в РФ у приватних інтересах, на шкоду інтересам країни та її громадян;

«Розпалювачів війни та військових злочинців», причетних до розв`язування агресивної війни проти України, її ведення, а також пропагандистської підтримки цієї війни, розпалювання ненависті до України та українців. Всього в базі станом на 02.11.2023 фігурує 1901 особи.

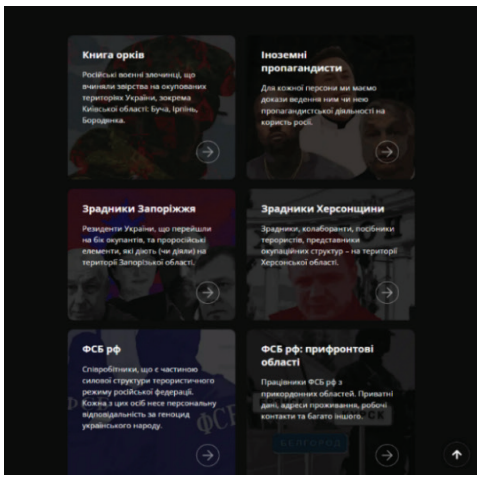
Список корупціонерів і розпалювачів війни – проект російського опозиціонера Олексія Навального та його команди.

Вони склали список осіб які причетні до збройного нападу росії на Україну, підтримують та виправдовують її.

Крім цього, відносно кожної особи наявні відомості про накладені санкції.



Вороги України від Molfar – чорний список осіб, які становлять загрозу національній безпеці України, що створений аналітиками OSINT-аґенції Molfar. За допомогою відкритих джерел інформації було створено список зрадників та ворогів України, а також зібрано докази скоєних злочинів та надано розширену інформацію по досліджених особах.



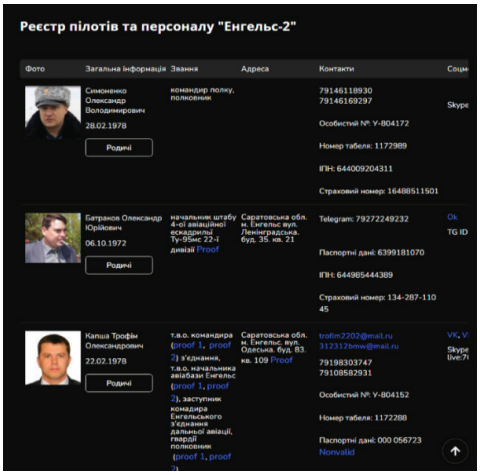
Так, на сайті можемо знайти таку інформацію:

Книга орків – російські воєнні злочинці, що вчиняли звірства на окупованих територіях України.

Іноземні пропагандисти – зібрані відомості про пропагандистську діяльність на користь росії іноземних лідерів громадської думки.

Зрадники Запоріжжя та Херсонщини – зрадники, колаборанти, посібники, представники окупаційної влади та інших структур, що перейшли на бік окупантів та діють на території тимчасово окупованих Запорізькій та Херсонській областях.

Випускники академії ФСБ, працівники ФСБ рф та окремо прифронтові області, ГРУ рф та СЗР рф – велика кількість інформації на співробітників, які несуть службу в силовому блоці окупантів.

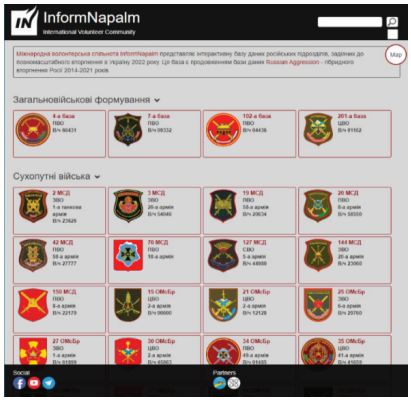


Пілоти російської авіабази «Енгельс-2» - російські пілоти та технічний персонал, які обслуговують стратегічні літаки на авіабазі «Енгельс-2» у Саратовській області, котрі є з учасниками військових операцій проти України.

Аґенція Molfar на базі створеної OSINT-спільноти збирає списки ворогів України з метою притягнення воєнних злочинців до відповідальності і надалі.

Підрозділи рф від InformNapalm - Міжнародна волонтерська спільнота InformNapalm створила інтерактивну базу даних російських підрозділів, задіяних до повномасштабного вторгнення в Україну 2022 року. Ця база є продовженням бази даних Russian Aggression - гібридного вторгнення Росії 2014-2021 років.

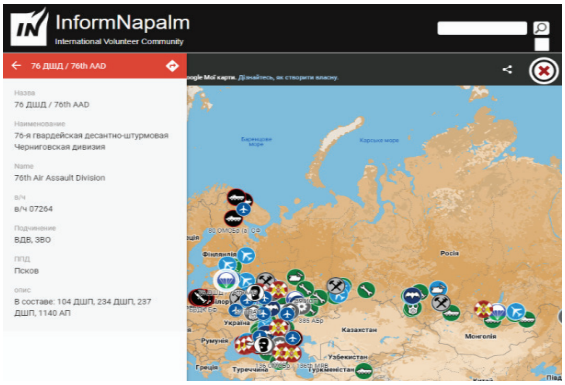
За допомогою неї можна визначити назву підрозділу, місце дислокації, № військової частини, військовий округ до якого відноситься підрозділ, склад, емблему, а також місця фіксації на території України.



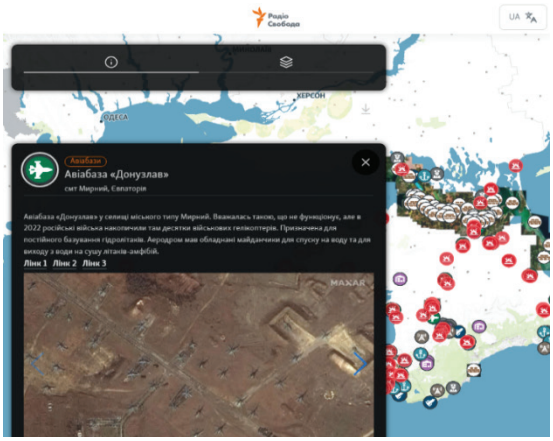


Крім цього, наявна карта із нанесеними на неї зазначеними підрозділами та відомостями по ним.

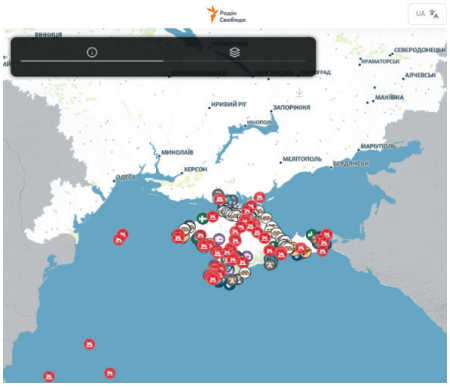


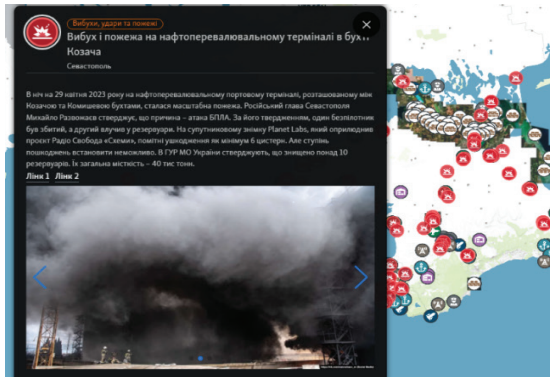


Карта військових об`єктів Криму – створена журналістами проєкту Радіо Свобода «Крим.Реалії» інтерактивна карта російських військових об'єктів в окупованому Криму – окопів, фортифікаційних споруд, а також місць вибухів та пожеж через ймовірні удари Збройних сил України по різних точках на Кримському півострові. Це стало можливим завдяки співпраці з командою іншого проєкту Радіо Свобода «Схеми», яка регулярно аналізує супутникові знімки ресурсу Planet Labs.



Всього зібрано 232 військові об`єкти в 10 категоріях із геолокаціями в Криму. На супутникових знімках Planet Labs і фото можна побачити бази Чорноморського флоту Росії, розташування військових частин різних родів військ, РЛС і ППО, аеродроми і паливні бази.





Відзначено понад 60 місць у Криму, де сталися вибухи з початку війни. Понад 60 еолокацій, де розташовані фортифікаційні споруди.

Чистилище – база даних осіб, в діях яких присутні ознаки злочинів проти національної безпеки України, життя та здоров'я людини , миру, безпеки людства та міжнародного правопорядку. База створена центром «Миротворець». Центр «Миротворець» здійснює свою діяльність у суворій відповідності до чинного законодавства України та міжнародних нормативно-правових актів, ратифікованих нашою державою.





Інформаційне наповнення сайту «Миротворець» здійснюється із загальновідомих та загальнодоступних відкритих джерел, які використовуються виключно у науково-дослідних, творчих та журналістських цілях.

Основними джерелами інформації, що використовуються Центром «Миротворець» для наукових досліджень, є відкриті для загального доступу матеріали, які друкуються та розміщуються в соціальних мережах, web-виданнях, на приватних web-сторінках, у спеціалізованих форумах та блогах, транслюються каналами телебачення та радіомовлення.

Центр «Миротворець» не заперечує проти використання інформації та відомостей, що містяться на однойменному сайті співробітниками СБ України, МВС України, Державної прикордонної служби України, ЗС України в оперативній та розшуковій діяльності.

ВЕБ-РЕСУРСИ ДЛЯ РОБОТИ ІЗ КАРТАМИ ТА ГЕОДАННИМИ

Робота з картами та геоданими в OSINT включає в себе збір, аналіз та використання географічних даних для отримання важливої інформації з відкритих джерел. Цей процес допомагає здобути більше контексту та розуміння щодо конкретних подій, локацій, об`єктів та їх взаємозв`язків. Нижче наведено деякі засоби та методи, які можуть бути використані при роботі з картами та геоданими в OSINT:

Супутникові знімки та карти: Використання супутникових знімків та карт, таких як Google Maps, Bing Maps, OpenStreetMap та інші, дозволяє отримувати детальні дані про локації, об'єкти, транспортні маршрути, географічні обмеження та інші важливі елементи.

Геотегінг і соціальні мережі: Аналіз геотегов та місцезнаходження, що додаються до фотографій, повідомлень у соціальних мережах та інших онлайн-ресурсах, може допомогти визначити місце перебування осіб чи об'єктів.

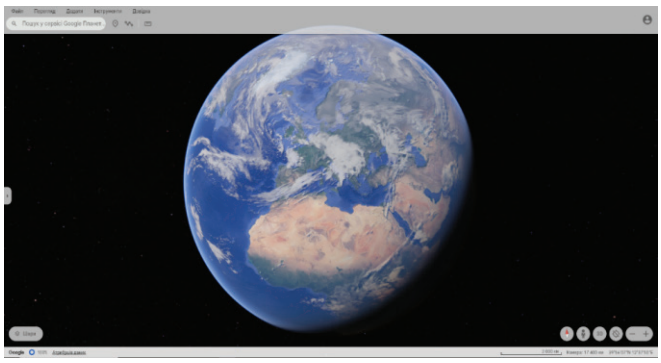
Геоінформаційні системи (ГІС): Використання спеціалізованих ГІС дозволяє аналізувати географічні дані, визначати географічні шаблони та візуалізувати інформацію на карті.

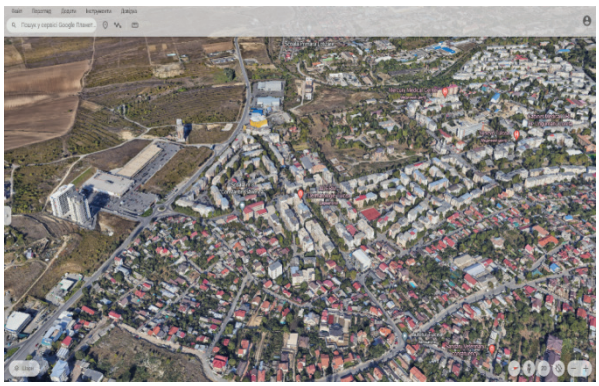
Аналіз транспортних мереж: Дослідження транспортних мереж, маршрутів руху, точок входу та виходу може допомогти в розумінні структури місцевості та потенційних шляхів переміщення осіб чи об'єктів.

Перехрестя даних з різних джерел: Комбінування геоданих з іншими видами відкритої інформації, такою як соціальні мережі, новини, публічні бази даних тощо, може допомогти у виявленні зв'язків та шаблонів, що сприяють розумінню контексту та ситуації.

Загалом, робота з картами та геоданими в OSINT дозволяє отримати глибоке розуміння географічного контексту та важливих об`єктів, що є важливим елементом в процесі збору та аналізу відкритої інформації.

Google Earth – проєкт компанії Google, у рамках якого в мережі Інтернет було розміщено супутникові (або в деяких точках аерофото-) зображення всієї земної поверхні. Фотографії деяких регіонів мають безпрецедентно високу роздільну здатність.

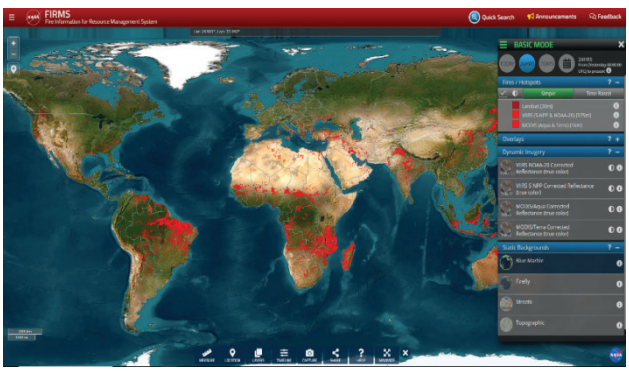




Google Earth автоматично завантажує з інтернету необхідні користувачеві зображення та інші дані, зберігає їх у пам'яті комп'ютера і на жорсткому диску для подальшого використання. Завантажені дані зберігаються на диску, і під час наступних запусків програми закачуються тільки нові дані, що дає змогу істотно економити трафік.

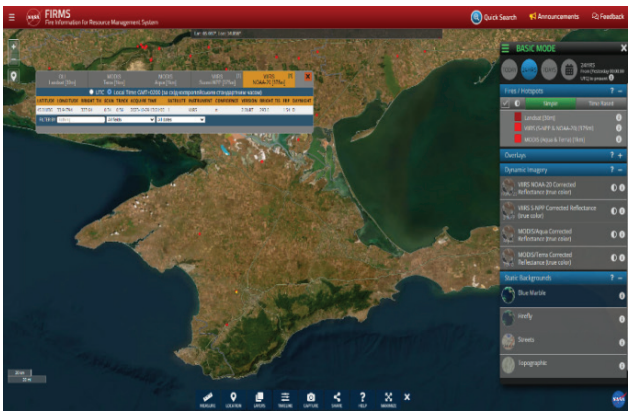
У програмі є шар «3D-будівлі» з тривимірними моделями, що додаються розробниками або самими користувачами за допомогою сервісу 3D Warehouse.

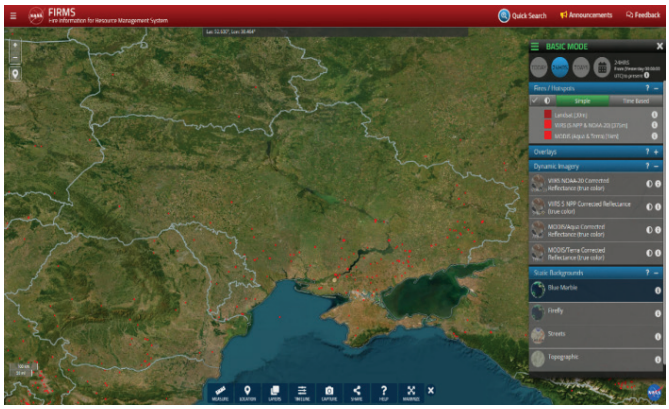
Firm NASA - надає активні данні про пожежі для моніторингу в режимі близькому до реального часу. Система пожежної інформації для управління ресурсами (FIRMS) поширює дані про активні пожежі в режимі близькому до реального часу (NRT) від спектрорадіометра з помірною роздільною здатністю (MODIS), встановленого на супутниках Aqua і Terra, та набору радіометрів для отримання зображень у видимому інфрачервоному діапазоні (VIIRS),



встановленого на супутниках S-NPP і NOAA 20 (офіційно відомий як JPSS-1). У глобальному масштабі ці дані доступні протягом 3 годин після супутникового спостереження, але для США і Канади активні виявлення пожеж доступні в режимі реального часу.

Дані про активні пожежі / осередки загоряння можна переглянути на карті FIRMS FIRE MAP або на сайті NASA`s WORLDVIEW, отримати сповіщення електронною поштою або завантажити



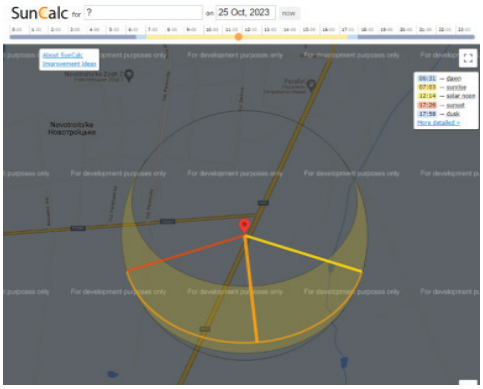


в наступних форматах: SHP, KML, TXT, WMS. FIRE DATA ACADEMY містить приклади аналізу та візуалізації даних про пожежі за допомогою Google Colaboratory (Colab), Jupyter Notebooks та Python.

Задопомогою даного сервісу можна проводити збір данних про ворожі обстріли, а також виявлення займань на ворожих позиціях.

SunCalc - калькулятор положення та фаз Сонця. Додаток для визначення курсу сонця в потрібний час і в потрібному місці за допомогою інтерактивної карти.

Використовуючи даний продукт, можна визначити час створення фото або відео, пору року, а також у взаємодії з іншим програмним забезпеченням і місце.



ТЕЛЕГРАМ-БОТИ ДЛЯ OSINT

Телеграм-боти в OSINT використовуються для автоматизації процесу збору відкритої інформації з різних джерел, таких як соціальні мережі, веб-сайти, форуми та інші. Вони надають зручний спосіб отримання інформації, яка може бути важливою для аналізу даних, проведення розслідувань або отримання розвідувальної інформації.

Основні ролі телеграм-ботів для OSINT включають:

Збір інформації: Телеграм-боти можуть автоматично збирати дані з різних джерел, що дозволяє отримати комплексну картину щодо конкретного об`єкта або події;

Аналіз даних: Деякі боти можуть аналізувати зібрану інформацію з метою виділення ключових фактів, зв`язків та інших важливих аспектів.

Відстеження змін: Телеграм-боти можуть вести постійний моніторинг об`єктів чи подій, інформуючи користувачів про будь-які зміни або нові дані;

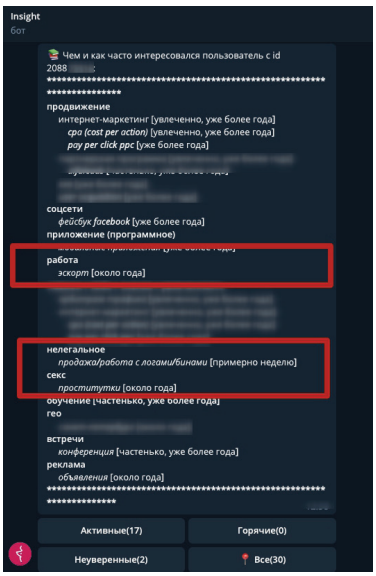
Сповіщення та повідомлення: Вони можуть надсилати сповіщення та повідомлення про важливі події або зміни, що допомагає оперативно реагувати на них;

Організація інформації: Телеграм-боти можуть допомагати у впорядкуванні та збереженні зібраної інформації для подальшого використання або аналізу;

Автоматизація завдань: Вони можуть автоматизувати деякі процеси збору та аналізу даних, що дозволяє ефективно використовувати час та ресурси.

Телеграм-боти можуть бути корисними для різних категорій користувачів, таких як дослідники, журналісти, розвідувачі, аналітики та інші, які потребують ефективних інструментів для збору та аналізу інформації з відкритих джерел.

Telesint_bot - дає змогу знаходити інформацію про те, в яких групах перебуває користувач. Пошук ведеться за власними базами і може бути не повним. Не плутайте групи з каналами. Щоб знайти інформацію про користувача, просто надішліть його ID, username, посилання на повідомлення у відкритій групі, контакт або просто перешліть повідомлення від нього. Бот спробує знайти їх у своїй базі та запропонує вам виконати пошук.



Ця інформація може розповісти про інтереси та захоплення особи, відностно якого проводиться моніторинг.

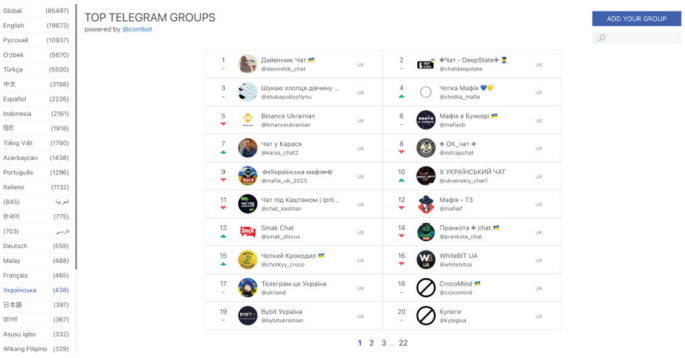
Кожному новому користувачеві дається за замовчуванням 3 запити.

MotherSearch - Аналог Google, але для Telegram. Допоможе знайти потрібний канал, текст, аудіо або документ.

GetContact - забезпечує доступ до функцій та можливостей популярного сервісу GetContact. GetContact є сервісом, який дозволяє користувачам знаходити та перевіряти інформацію про власників телефонних номерів.

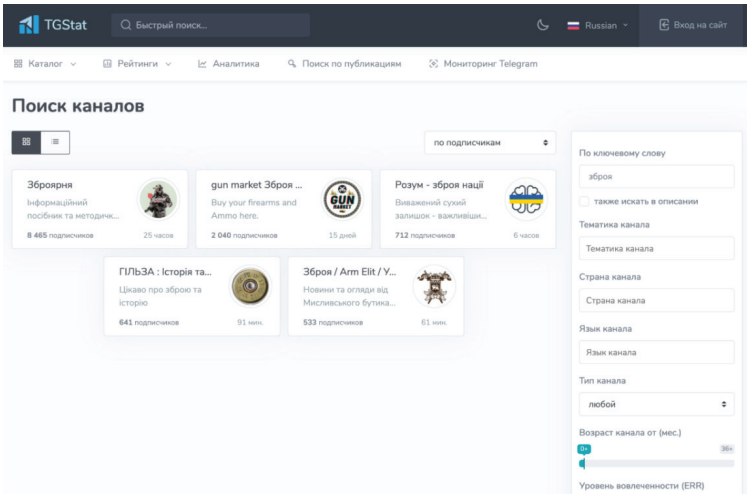
Smart_SearchBot - платний сервіс-бот для пошуку інформації по ФІО, номеру телефону, авто, фото, Email або ID. За допомогою доступу до баз ГІБДД, РСА, історії Авто.ру, Дром.ру та іншим утечкам Smart_SearchBot може знаходити людей, пошту, оголошення, фотографії та соціальні мережі.

Combot.org представлено каталогом чатів Telegram з функціями додавання вмісту особистих чатів та групування по країнах, виходячи з мови, на яких ведуться канали. В наявності швидкий пошук, результати якого виводяться паралельно із введенням запиту та рейтинг.



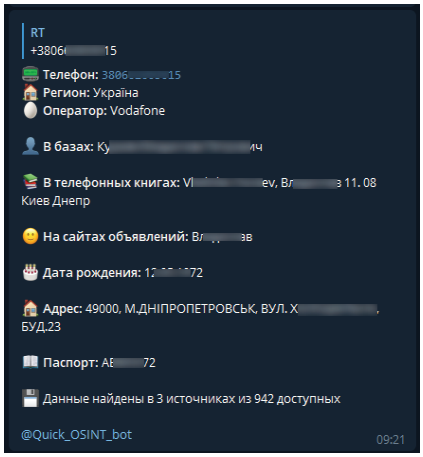
Tgstat вважається основним (не офіційним) інструментом пошуку каналів в Telegram. Групує список за:

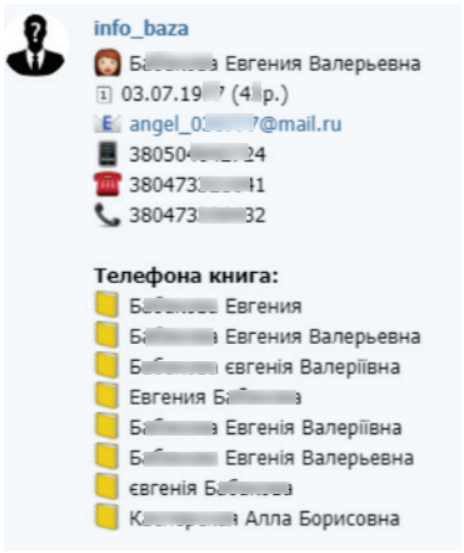
- *ключовими словами;*
- *тематиці (декілька десятків варіантів);*
- *країні (декілька десятків варіантів);*
- *мовах (англійська, узбецька, українська, казахська, білоруська, російська);*
- *типу канала (будь-який, публічний, приватний).*



Також є можливість переглянути рейтинг, аналітику каналів, чатів, публікацій, а також здійснити пошук по публікаціях. Щоб знайти осіб в Телеграмі, існує декілька варіантів: *за номером телефону; за юзернеймом; за прізвищем, ім'ям; з допомогою ботів.*

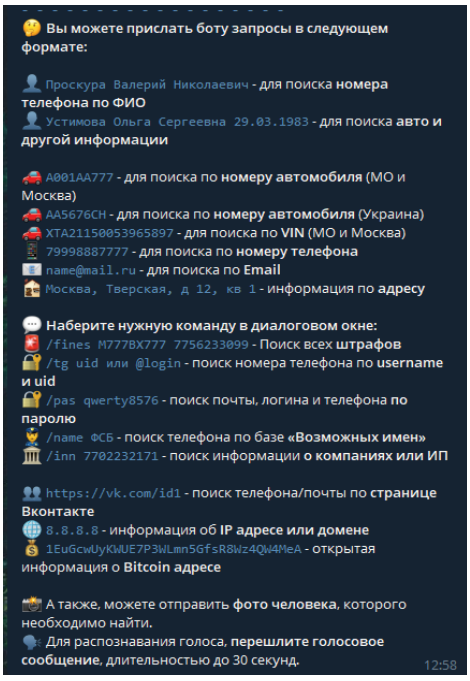
quick_osint_0_bot здатний шукати по телефону, адреси електронної пошти, державний номеру або VIN номеру автомобіля, номер паспорта, ІПН тощо. Цікава особливість – пошук за паролем: бот шукає в злитих базах email, якому може відповідати заданий пароль. Також є пошук по фото.





InfoBaza (назва боту періодично змінюється, а також доступ можливо отримувати через підключення свого власного боту) містить інформацію щодо номерів телефонів, адресу електронної пошти, персональних даних (ПІБ, дата народження і тощо), як людина підписана в інших тощо.

Oko39boga_bot (назва боту періодично змінюється, а також є особливість доступ можливий після передачі боту абонентського номеру профілю Телеграм, при чому абонентам із українськими номерами доступ отримати не можливо). Зазначений бот має такий набір функцій: пошук по імені в простому текстовому форматі, за номером автомобіля, за номером телефону, за адресою електронної пошти, за назвою юридичної особи, ІПН, сторінкою в соціальній мережі або месенджері тощо.



HimeraSearch - працює як із відкритими джерелами інформації OSINT, так і із закритими HUMINT (викупленими конфіденційними). Список функцій внушальний: перевірка номера, перевірка ФО, перевірка E-mail, пошук по Авто, пошук по паспорту, перевірка ІНН ЮО, пошук по ІНН, пошук по СНІЛС, Скоринг ФО, пошук по ФОТО, перевірка адреси.

DataLeakBot - пошук доступний по E-mail, номеру, ПІБ, адресі тощо. За придбану преміум підписку надає більше інформації. Для журналістів, рослідувачів чи представників державних органів є додаткова можливість доступу до веб-інтерфейсу даного інструменту.

DataSearcherBot - може лише за частиною ім'я і дати знайти людину, безкоштовно він показує інфу (від ІПН, паспорт, телефон до адреси) за зірками. Наприклад: Петренко Ірина Пет******, +38066316*, але знову ж таки якщо ви знаєте прізвище, ім'я і дату то встановити по-батькові буде легко.

Глаз Бога - російський бот, який пробиває інформацію за фото, номером телефону, адресою, акаунтами у «Вконтакте», «Одноклассниках», у Телеграмі та іншими параметрами.

Бот збирає інформацію з відкритих джерел (відкриті сторінки в соцмережах, акаунти в месенджерах). У ньому міститься частина того, що людина залишила про себе за роки в інтернеті. Плюс у ньому є інформація з поширених витоків із великих сайтів: «Яндекс доставка», «Мамба.ру», «Вконтакте», last.fm тощо.

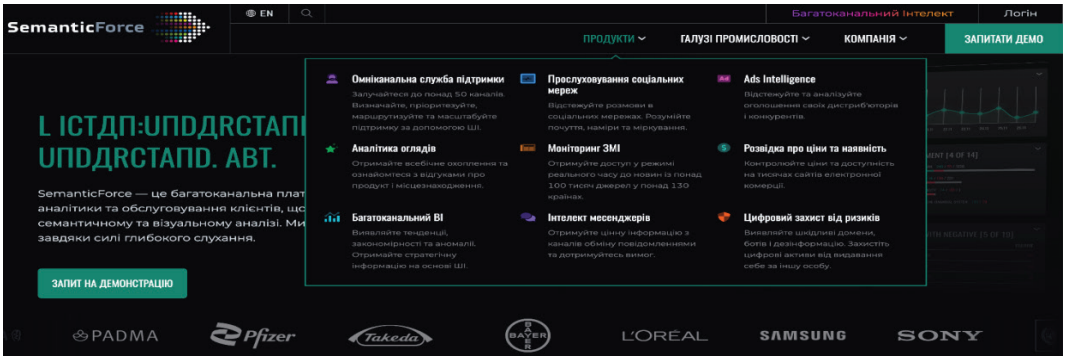
Під час першого запуску бота ви передаєте йому свій номер, який, очевидно, вноситься в базу бота. Телефонний номер буде видно в пошуку, якщо користувач не оплатив підписку на бот. Крім того, якщо ви оплатите бот, він збереже зазначену вами електронну пошту. Також бот збирає інформацію про приблизне місцезнаходження користувачів, які запускають бот. **Тому не забувайте подбати про інформаційну безпеку!**

Розробник бота «Глаз Бога» не приховує, що дає безкоштовний доступ до бота російським силовикам.

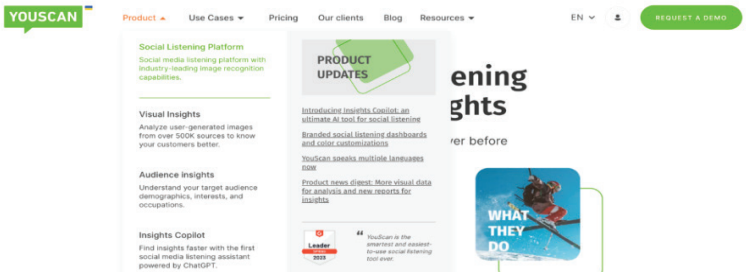
GetFB - бот працює дуже просто: за введеним номером мобільного телефону в міжнародному форматі (+7XXXAAABBCC) GetFB знаходить зареєстровану на цей телефон сторінку у Facebook. Грошей за свою роботу бот не просить і працює чудово.

ІНСТРУМЕНТИ МЕДІА-МОНІТОРИНГУ

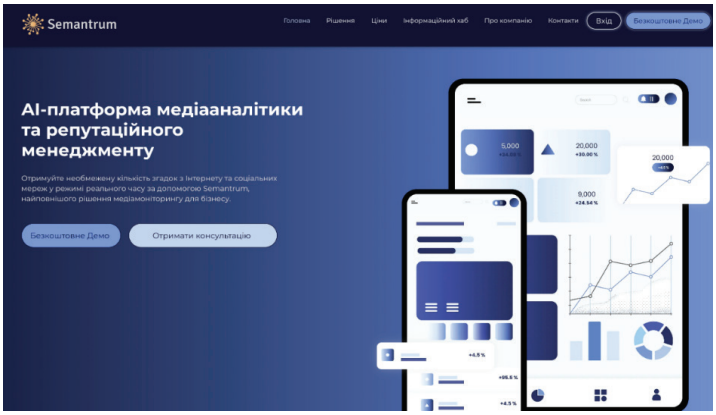
SemanticForce – це багатоканальна платформа для медіа-моніторингу та аналітики, що базується на розширеному семантичному та візуальному аналізі медіоконтенту.



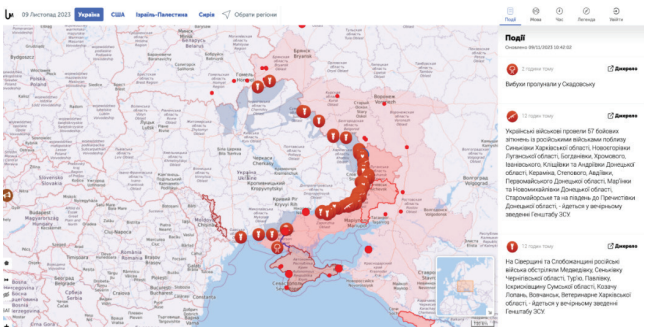
YouScan – платформа з моніторингу та аналітики соціальних медіа та онлайн-ЗМІ, яка працює на основі штучного інтелекту та має провідні можливості розпізнавання зображень, допомагає заздалегідь вивчати думки користувачів, знаходити важливі інсайти та управляти репутацією.



Semantrum – AI-платформа медіааналітики та репутаційного менеджменту, завдяки якій можна отримати необмежену кількість згадок з Інтернету та соціальних мереж у режимі реального часу 24/7 з 50 000+ українських та міжнародних веб-джерел, а також ТБ, відео-хостінги (YouTube), радіо, преса та соціальні мережі (Facebook, Twitter, Instagram, Telegram та ін.).

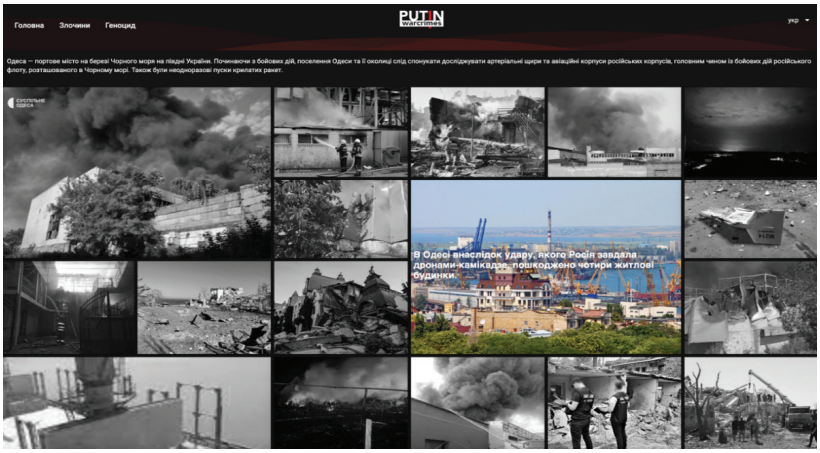


Онлайн-ресурс новин **Liveuamap** надає інформацію про події в онлайн режимі з відображенням її на карті світи.



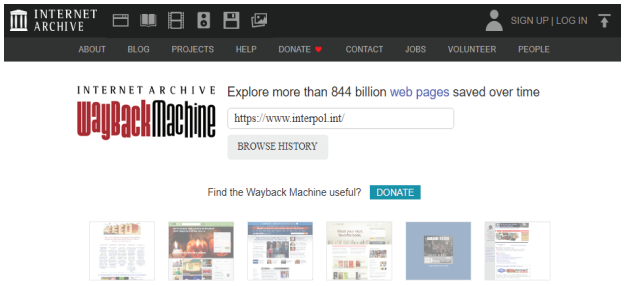
Cyberwar.liveuamap аналогічно ресурсу Liveuamap надає інформацію про події в онлайн режимі з відображенням її на карті світу тільки за категорією «кібервійна»

PutinWarCrimes – електронний сервіс-галерея, мета якого є висвітлення злочинів російських окупантів на території України. Сервіс представляє собою динамічний веб-сайт, на якому розміщено фото-контент з коротким описом про факти, що підтверджують злочинні дії рф. Сервіс містить 29 категорій за регіонами (Одеса, Київ, Львів, Харків та інші). Джерелами вказаних даних є будь-яка інформація з офіційних відкритих джерел та інформація, отримана з офіційних запитів.



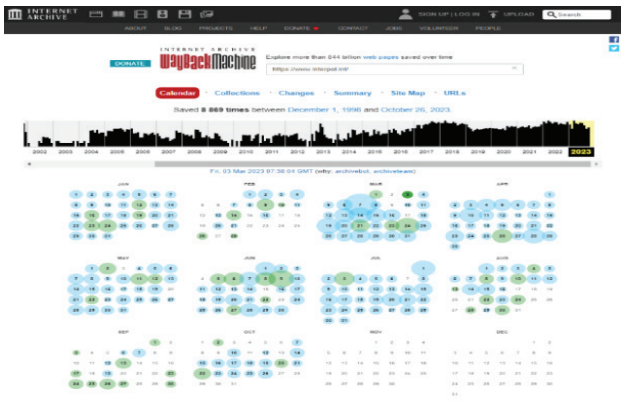
ІНШІ ЗАСТОСУНКИ ДЛЯ ВИКОРИСТАННЯ В АНАЛІТИЧНІЙ ДІЯЛЬНОСТІ

Wayback Machine - безкоштовний онлайн-архів некомерційної бібліотеки «Архів Інтернету». За допомогою пошукових роботів Wayback Machine архівує і робить загальнодоступною більшу частину «відкритого» інтернету.

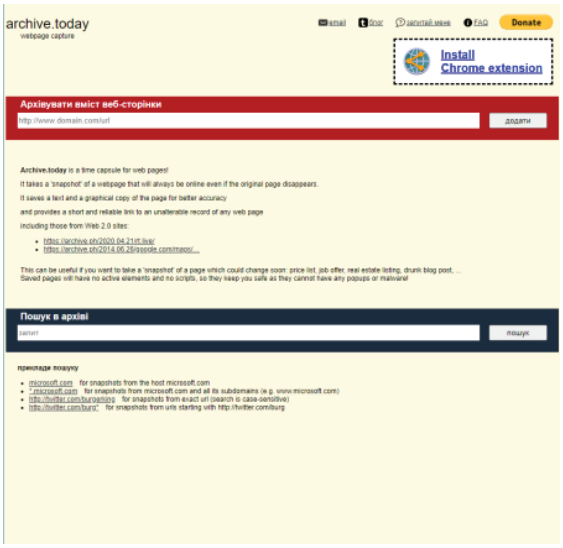


Із запуском Wayback Machine «Архів Інтернету» став одним із найпопулярніших і найвпізнаваніших онлайн-порталів і головним сервісом веб-архівування.

У 1999 році «Архів» почав розширювати колекцію за межі архівного веб-контенту, щоб забезпечити статус як до оцифрованих, так і до цифрових ресурсів, зокрема книжок, аудіо, фільмів, зображень, документів, програмного забезпечення та відеоігор. Деякі сканування виконуються пошуковими роботами самого архіву, а інші - партнерськими організаціями. Окремі бази даних можуть купуватися за рахунок пожертвувань користувачів і цільових придбань. Самі творці організації порівнювали свою колекцію з Олександрійською бібліотекою. На 2023 рік Wayback Machine містив близько 828 млрд веб-сторінок - більше, ніж документів у Бібліотеці Конгресу.



Archive.today - це капсула часу для веб-сторінок. Вона робить «моментальний знімок» веб-сторінки, який завжди буде доступний в Інтернеті, навіть якщо оригінальна сторінка зникне.



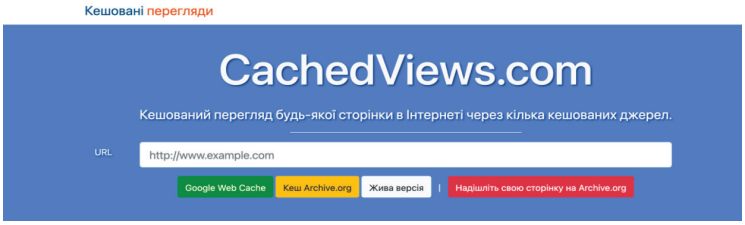
Він зберігає текстову та графічну копії сторінки для більшої точності і надає коротке і надійне посилання на незмінний запис будь-якої веб-сторінки в тому числі з сайтів Веб 2.0. Це може бути корисно, якщо ви хочете зробити «знімок» сторінки, яка може скоро змінитися: профіль в соц.мережі, публікація, повідомлення, веб-сторінка та інші.

Збережені сторінки не матимуть активних елементів і скриптів, тому вони забезпечують вашу безпеку, оскільки не містять спливаючих вікон або шкідливого програмного забезпечення!

Ресурс **archive.org** – це інтернет-архів, який містить 859 мільярдів веб-сторінок, збережених за останні 20 років. Дає доступ до зображень, відео, таблиць стилів, сценаріїв та інших веб-об'єктів і посилаються на них.

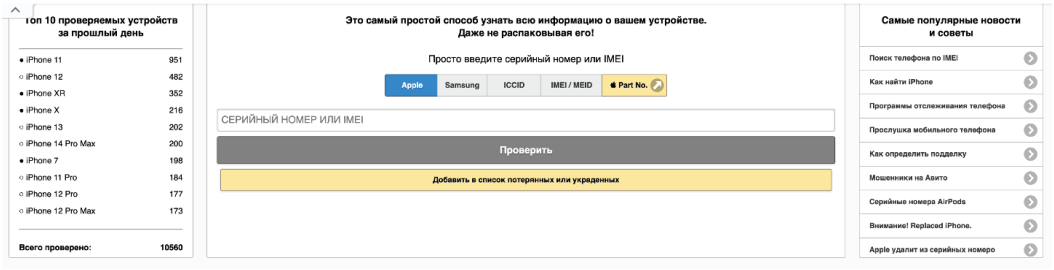


Cachedviews – це сервіс з пошуку копій веб-сторінок, збережених у кеші Google. Принцип дії: Google Bot сканує Інтернет і створює резервну копію на випадок, якщо поточна сторінка недоступна. Потім ці сторінки стають частиною кешу Google, в середовище якого можна здійснити пошук. Особливо корисні коли сайт тимчасово не працює або необхідно переглянути історію веб-сайту. Є безкоштовним сервісом, термін оновлення декілька днів.

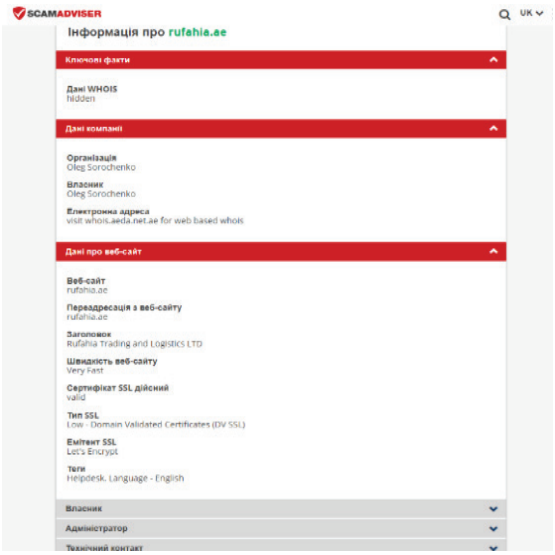


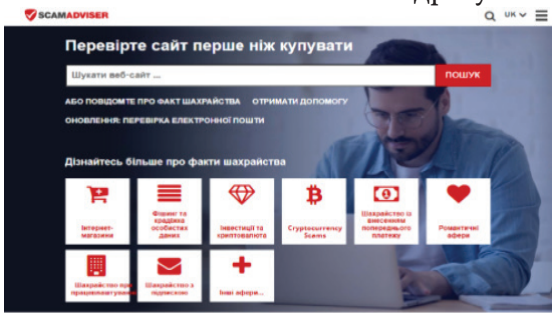
HTTrack – це безкоштовна утиліта для браузера в режимі офлайн, яка дозволяє завантажувати веб-сайт з Інтернету в локальний каталог, рекурсивно створюючи всі каталоги, отримуючи HTML, зображення та інші файли з сервера на ваш комп'ютер. HTTrack організовує відносну структуру посилань оригінального сайту. Для використання необхідно відкрити сторінку «дзеркального» веб-сайту в своєму браузері, і буде можливість переглядати сайт від посилання до посилання, анологічно перегляду його онлайн. HTTrack також може оновити існуючий дзеркальний сайт і відновити перервані завантаження.

SNDeepInfo – це сервіс перевірки серійних номерів телефонів, смартфонів, фотоапаратів, побутової техніки, imei телефонів усіх марок та іншої електронної та побутової техніки. За допомогою сервісу можна отримати розширену інформацію із зазначенням фізичних та технічних характеристик: колір пристрою, обсяг пам`яті, дату виробництва, версію прошивки при продажу пристрою, способи розблокування.



Scamadviser - використовує понад 40 джерел даних для перевірки сайтів. Від IP-адреси веб-сервера, наявності контактної інформації на сайті, віку URL-адреси, рейтингів на сайтах відгуків і багато іншого. За допомогою даного сервісу є можливість визначити власника та адміністратора, а також IP-адресу.

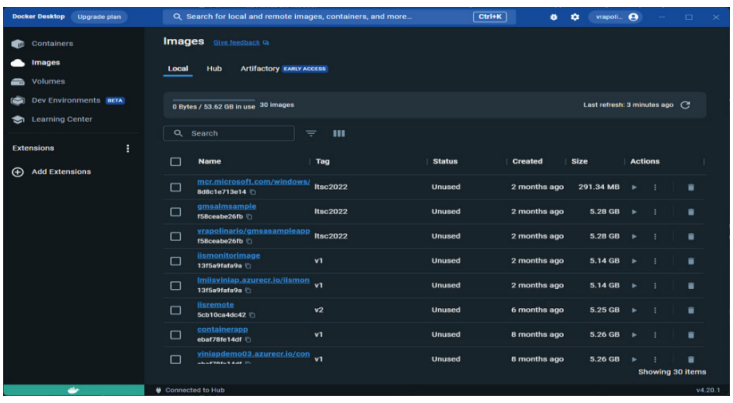




LibreOffice - потужний офісний пакет; завдяки його простому інтерфейсу і потужним інструментам Ви розкриєте свій творчий потенціал і підвищите продуктивність.

LibreOffice містить кілька програм, які роблять його найпотужнішим безкоштовним і відкритим пакетом офісних програм на ринку: текстовий процесор Writer, програма для роботи з електронними таблицями Calc, рушій презентацій Impress, Draw, наша програма для малювання та блок-схем, Base, наша база даних і інтерфейс бази даних, а також Math для редагування математичних виразів. Використовуючи таблиці Calc, можна легко працювати із таблицями формату .csv.

Docker - програмне забезпечення, що дозволяє автоматизувати процес розгортання та керування додатками в середовищах, які підтримують контейнеризацію. Воно виступає як контейнеризатор додатків, дозволяючи «упакувати» додаток разом з усіма його залежностями в контейнер. Цей контейнер може бути розгорнутий на будь-якій системі Linux з підтримкою контрольних груп у ядрі. Також воно надає набір команд для управління цими контейнерами.



DOI: https://doi.org/10.36486/978-966-2310-66-5-17

Скоро залишаться лише дві групи працівників: ті, хто контролює комп'ютери, і ті, кого контролюють комп'ютери. Постарайтеся потрапити в першу.

Дейв Баррі

РОЗДІЛ 17
Сучасні пошукові сервіси та інструменти аналізу кіберзлочинів

Карен Ісмайлов
Євгеній Панченко

ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-ПОШУКОВОЇ СИСТЕМИ GOOGLE

Google пропонує користувачам всесвітньої мережі велику кількість сервісів і послуг, що при правильному використанні стають вагомим аргументом як в руках правоохоронних органів, так і зловмисників.

Сервіси Google, за допомогою яких проводиться пошук оперативної інформації:

- *Google Статистика пошуку дозволяє дізнатись найбільш популярні, а також ті, які швидше за все набирають популярність, запити в заданий відрізок часу.*
- *Blogger – це сервіс для ведення блогів, що дозволяє тримати на своєму хостингу не тільки програмне забезпечення, а всю інформацію: записи, коментарі та персональні сторінки в СУБД на серверах Google.*
- *Google Docs – веб-орієнтований застосунок для роботи з документами, що допускає спільне використання документа. Зараз замінений на Google Drive.*
- *Google Drive – хмарне сховище від Google з можливістю онлайн (в браузері) перегляду безлічі типів файлів (у тому числі і файлів фотошопу). Документи також можна редагувати і створювати в Google Docs. Пропонується 5 Гб вільного місця у безкоштовному тарифі.*
- *Gmail – безкоштовна електронна пошта з великим обсягом місця для зберігання повідомлень (понад 10,1 Гб), з доступом по POP3 і зручним веб-інтерфейсом. Також є OpenID-провайдером для всіх служб Google.*
- *Google Maps – набір карт, побудованих на основі безкоштовного картографічного сервісу.*
- *YouTube – відеохостинг.*
- *Google+ – соціальна мережа.*

Спеціальний пошук Google:

- *Google Images – сервіс пошуку картинок в пошуковій системі Google.*
- *Google SSL – безпечний пошук від Google. Зв'язок між користувачем і сервером здійснюється по зашифрованому каналу, що виключає можливість перехоплення інформації користувача третіми особами.*
- *Google Suggest – частина пошуку Google, технологія автозаповнення рядка пошукового запиту на основі загальної статистики найпопулярніших запитів.*
- *Google Video – сервіс для пошуку, перегляду і збереження відео.*

Пошукові машини Google дозволяють працювати не тільки на вебсайтах, а й у більш вузьких джерелах інформації.

Google проіндексував більше HTML-сторінок в Інтернеті, ніж будь-який інший пошуковик. З'явилися функції пошуку по телефонних номерах, адресах, словниках і довідниках. Пізніше Google пішли ще далі. І тепер є можливість шукати на Google новини, патенти, статті в журналах, картинки, книги, відеоролики і багато іншого.

Інструменти:

- *Google Earth – модель планети Земля, створена за допомогою супутникових знімків.*
- *Google Web Accelerator – програма, що прискорює роботу браузера шляхом кешування та попереднього скачування інформації, що, можливо, буде цікавити користувача. Програма використовує проксі-сервери, що належать Google.*

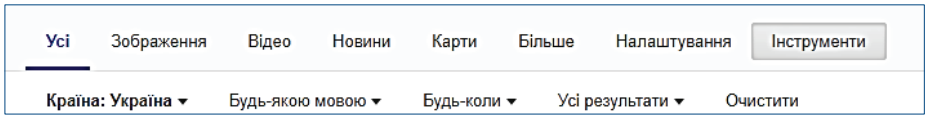
Оскільки пошукова система компанії Google користується найвищою популярністю серед користувачів мережі інтернет, вона накопичує величезну кількість інформації про організації користувачів, які навіть не здогадуються, що своїм серфінгом вони залишають велику кількість слідів.

> *Головним завданням правоохоронця є уміння своєчасно знаходити ці сліди, аналізувати їх і вживати заходів превенції і розкриття злочинів.*

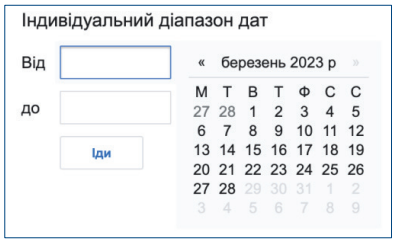
Інтерфейс системи Google досить зручний у користуванні, зрозумілий та функціональний. Пошукова система Google знаходить інформацію за допомогою пошукових роботів Googlebot. Саме вони отримують запит, введений користувачем у пошукове поле. Роботи сканують мільярди сторінок, використовуючи для цього велику кількість комп'ютерів. Googlebot працює автоматично та самостійно визначає, які сайти сканувати, як часто це робити та яку кількість сторінок потрібно вибрати на кожному з них. Для початку робот перевіряє список сторінок, створений на базі попереднього сеансу сканування, доповнює даними із файлів Sitemap, переглядаючи ці сайти він знаходить посилання (SRC та HREF) і після цього також додає до списку.

Для звичайного пошуку інформації потрібно відкрити браузер у полі пошукової системи, ввести запит, натиснути клавішу пошуку, і знайти потрібну інформацію в результатах пошуку. Але звичайний пошук не задовольняє потреби правоохоронних органів. Звісно, що на сторінці звичайного пошуку присутні деякі інструменти.

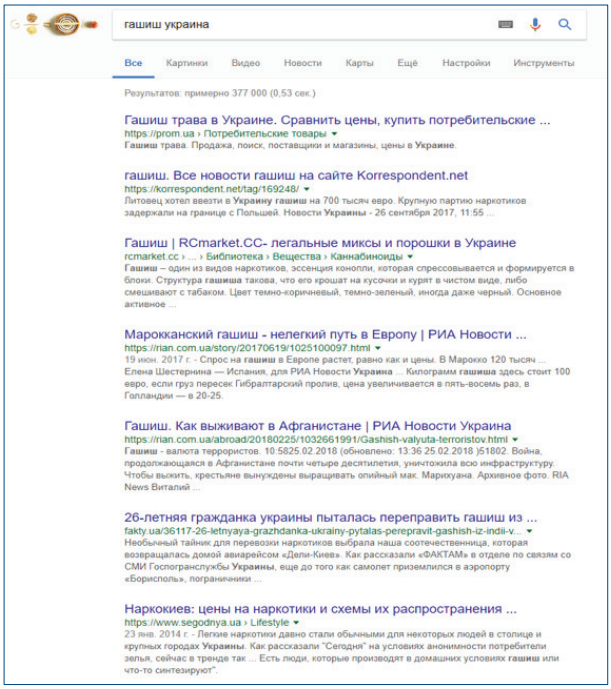
На панелі під пошуковим полем доступні такі інструменти як: вибір країни; вибір мови; вибір періоду публікування; вибір усіх результатів або дослівно.



Найкориснішим інструментом з цього набору є вибір періоду, за який потрібно отримати результати. Проте, перелік цих інструментів обмежений, та здійснення необхідної фільтрації через них є неможливим.



Найбільш ефективним результат пошуку буде за допомогою розширеного пошуку або вводом у базовий пошук структурованого запиту. Також цей метод пошуку використовується для неіндексованих сторінок. Сторінки можуть бути неіндексовані так як пошуковий робот ще не дістався цієї сторінки, або адміністратор сайту заборонив індексування сторінки пошуковими системами у файлі robots.txt.



На зображені приклад звичайного пошуку, пошуковий робот отримав простий запит у вигляді двох ключових слів. Відповідно він шукає інформацію даного запиту і відображає результати, знайдені на всіх сайтах у всіх документах. Такий пошук вважається менш ефективним та займає більше часу. Адже користувач сам аналізує велику кількість інформації та відокремлює потрібну.

Структуровані запити використовуються у пошукових системах, що підтримують логічні оператори, наприклад EGoogle. Вони створені для уточнення та сортування інформації відповідно до пошукового запиту і пошук здійснюється за допомогою певних символів та слів, що відображені в таблиці.

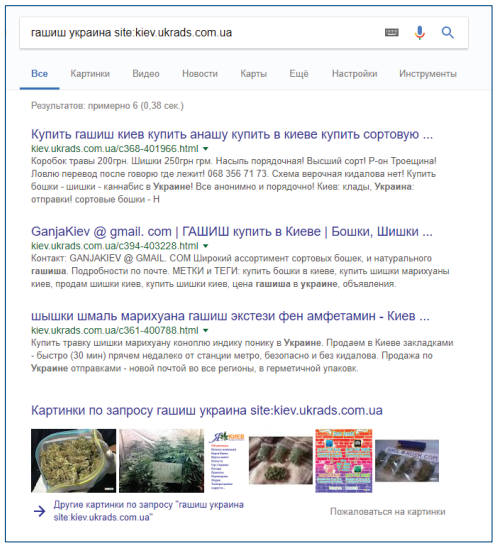
Оператори пошуку + знання джерел + ключові слова дають в сумі «смарт-запити». *Приклади:*

- filetype:»xls | xlsx | doc | docx | ppt | pptx | pdf» site:.co.ua
- intitle:»Олександр Галушко» site:facebook.com
- intitle:»база даних» site:olx.ua
- ПЛР-тест AND коронавирус AND паспорт вакцинації site:olx.ua
- «Scanned by Camscanner» filetype:pdf site:mil.ru
- site:amazonaws.com filetype:sql
- site:https://docs.google.com/spreadsheets/d/.

Таблиця 17.1. Базові пошукові оператори системи Google

ОПЕРАТОРИ	ЗНАЧЕННЯ
AND / +	Оператор за замовчуванням – кожен пробіл у полі пошуку
OR / |	Використовується для пошуку схожого чи дотичного контенту
NOT (-)	Виключає непотрібні слова з пошуку
«»	Знаходить контент, що містить зазначену послідовність ключових слів
filetype:	Звужує пошук до певного типу контенту
site:	Звужує пошук до певного домену чи піддомену
intitle:	Звужує пошук до заголовків вебсторінок
allintitle:	Шукає заголовки, що містять усі задані слова чи фрази
inurl:	Звужує пошук до URL-адрес вебсторінок
allinurl:	Шукає URL-адреси, що містять кілька заданих слів чи фраз
intext:	Пошук лише в тексті сторінки
allintext:	Пошук сторінок, що містять всі зазначені слова чи фрази в тексті
before: / after:	Звуження пошуку до певного часового періоду
wild card (*)	Шукає інші написання слова, слова з іншими закінченнями тощо
cache:	Оператор видає останню кешовану версію вебсторінки
related:	Видає вебсайти, які Google вважає схожими на те, що ви шукаєте

Разом із цим, так як багато користувачів не володіють технологією використання операторів, інформаційно-пошукові системи пропонують своїм клієнтам спеціальні форми з метою спростити завдання формування складних запитів. Викликається така форма у результаті клацання на кнопці Розширений пошук (Advanced search, Search Assistant), приклади використання якої у службовій діяльності поліцейського будуть наведені нижче.



Однак слід зазначити, що пошук інформації методом структурованого запиту досить простий і ефективний. Застосовується він досить легко. Наприклад, для того щоб здійснити пошук на окремому сайті, потрібно ввести у пошукове поле звичайний запит, додати до нього оператор site:, та вказати сайт на якому потрібно здійснити пошук.

В пошукове поле введено структурований запит, а саме: використано оператор site:... Отримавши таку команду, Googlebot починає сканувати заданий сайт на наявність введеної інформації в запит. Отже, у підсумку видно, що результати звичайного пошуку – це переважно новини.

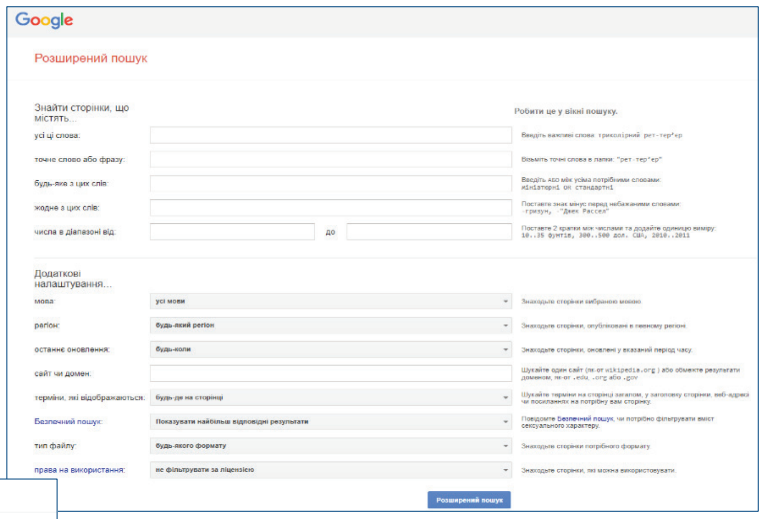
Для того, щоб знайти потрібну інформацію, працівнику правоохоронних органів потрібно буде відсіювати майже всю інформацію цієї сторінки та переходити до іншої. Зі структурованим пошуком ситуація зовсім інша. Наприклад, в результатах наведені оголошення про продаж наркотичних засобів, у даній ситуації правоохоронець може переходити за посиланням та продовжувати пошук інформації вже безпосередньо на сайті.



Слід відмітити, що ця функція є досить корисною для пошуку по інших сайтах, так як у багатьох сайтів пошукова система працює гірше, ніж Google.

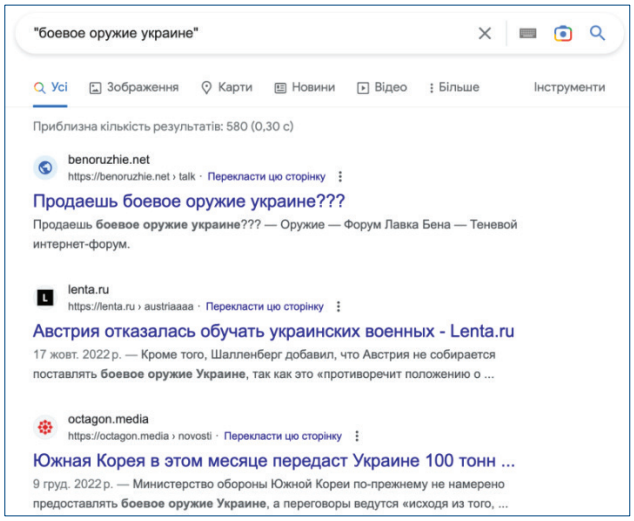
Автоматизоване використання операторів Google міститься на сайтах Advangle, DorkSearch і аналогічних. Дані ресурси працюють з допомогою штучного інтелекту та значно прискорюють роботу.

У випадку, коли правоохоронець не володіє достатнім рівнем знань про пошукові оператори, але йому потрібна інформація з високим рівнем деталізації, йому буде корисною функція розширеного пошуку Google. При переході до розширеного пошуку користувач потрапляє на сторінку, що містить кілька полів пошуку з визначеними параметрами.



Пошук за словами опрацьовує окремо усі задані слова в полі «Усі ці слова» (звичайний пошук).





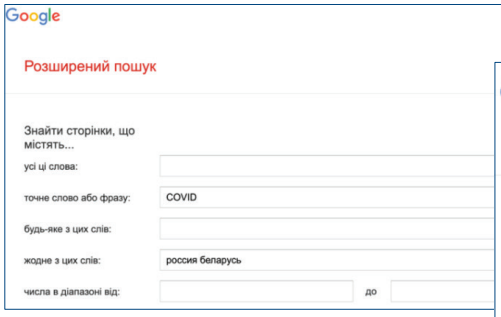
Пошук по точній фразі або слову дозволяє знайти конкретну фразу, у якій слова йдуть підряд. У пошуковому полі введений запит буде взятий у лапки.

Лапки допомагають у тому плані, що прибирають з результатів велику кількість непотрібних посилань.

За таким механізмом виконується пошук номерів телефонів або поштові скриньки з різним варіантом написання.

Якщо запит складається з кількох слів, при введені в поле «будь-яке з цих слів» у результаті буде будь-який запит, у якому присутнє будь-яке слово із запиту.

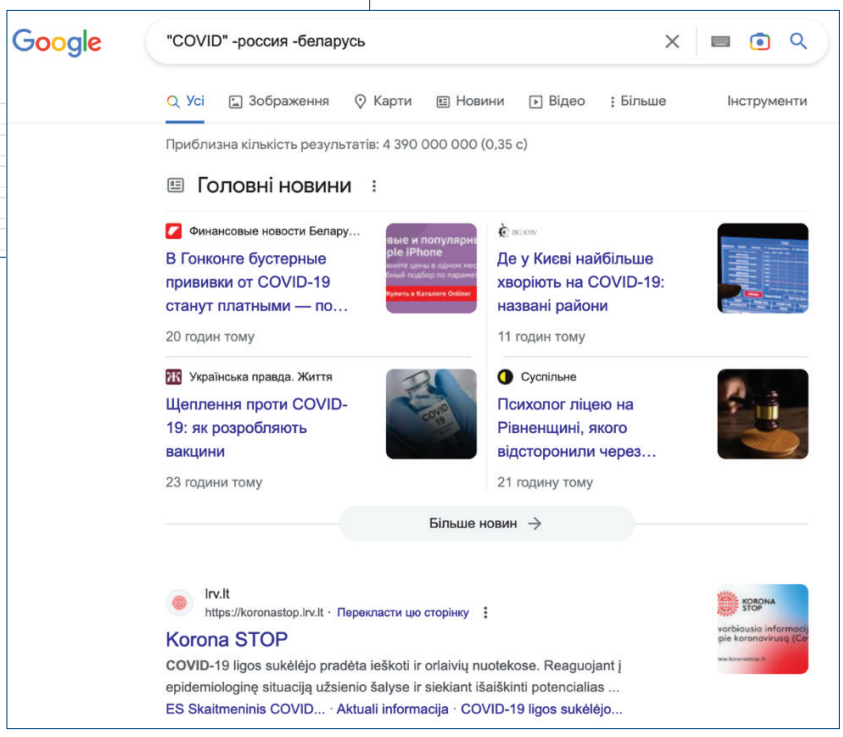
Комплексний пошук



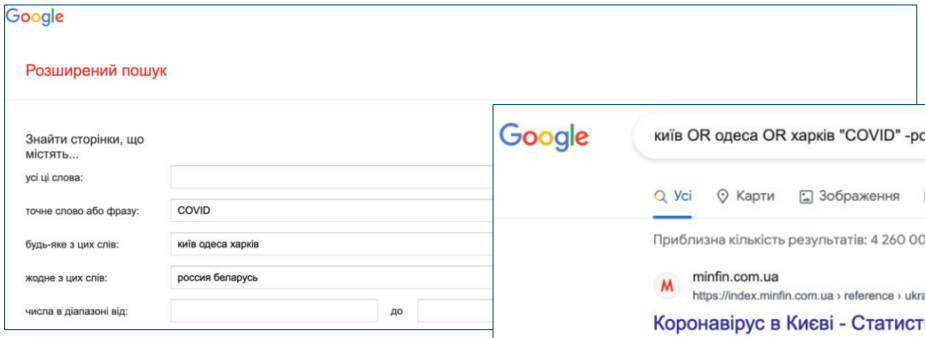
Комплексний пошук, «жодне з цих слів» допомагає виключити слово з результатів пошуку.

Логічний оператор (АБО) заощадить час та допоможе отримати всі результати, якщо є кілька варіантів написання ключового слова, яке потрібно знайти.

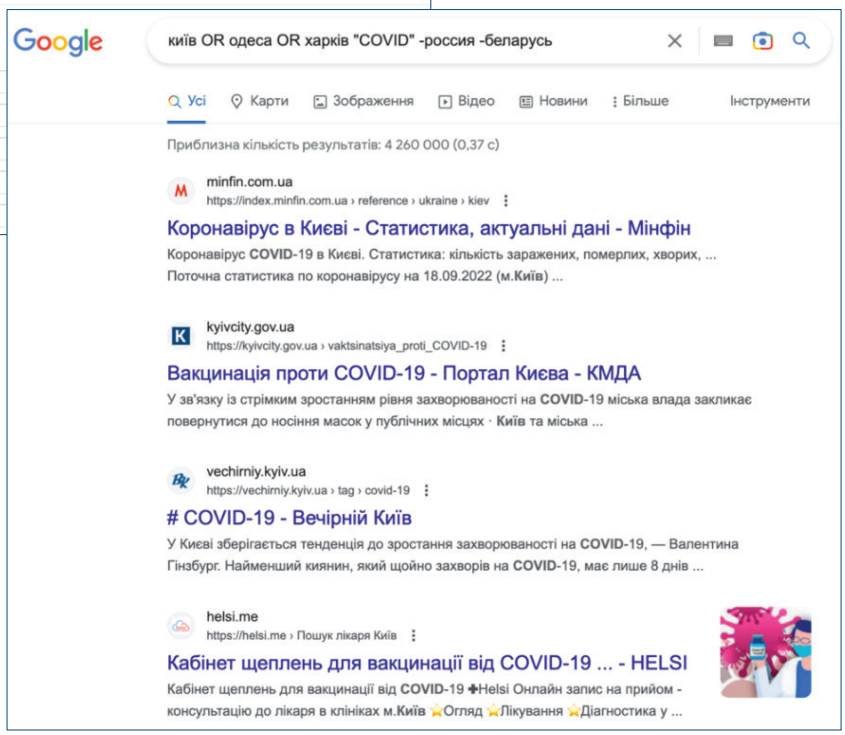
Результати комплексного пошуку



Логічний оператор АБО (OR)



Результати використання логічного оператора «АБО»



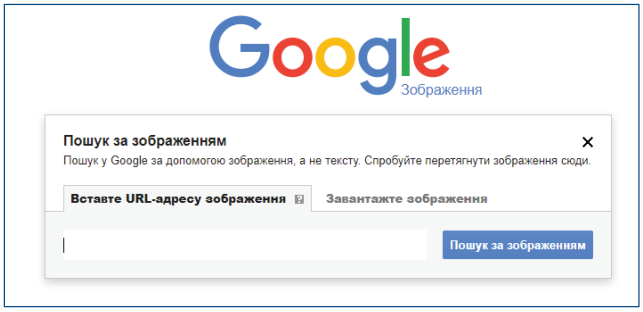
ПОШУК ПО ФОТО

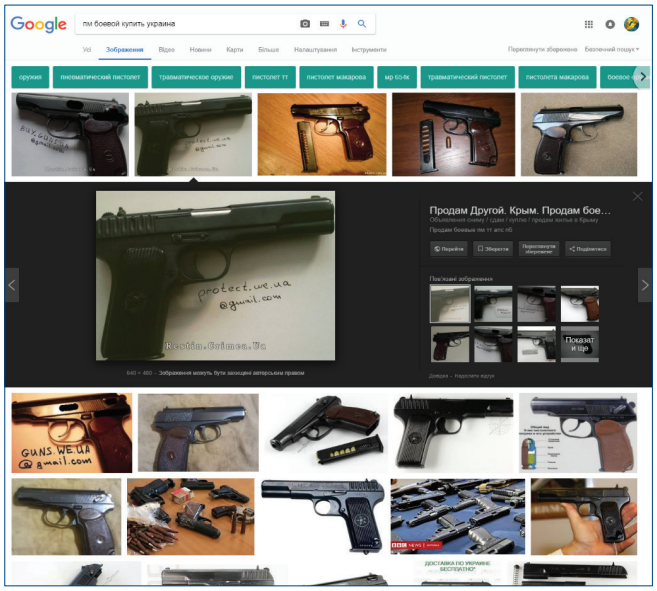
Серед сервісів Google існує досить корисна функція, яка при правильному використанні дає можливість ефективно здійснити пошук оперативної інформації маючи фото. Інтерфейс даного сервісу майже не відрізняється від звичайного пошуку. Єдина відмінність – це під лого Google напис «зображення», яке зявляється лише при заданні запиту та отриманні результатів. Для пошуку використовується як фото, так і текст, але пошук буде здійснено серед зображень та користувач отримає результати пошуку у формі зображень.

Пошук по зображенню

Для пошуку по зображенню є два варіанти вводу запиту: перший – це введення тексту в поле пошуку, а другий – за зображенням. За зображенням потрібно натиснути на іконку камери потім вибрати один з варіантів – або вказати посилання (якщо фото розташоване в інтернеті).

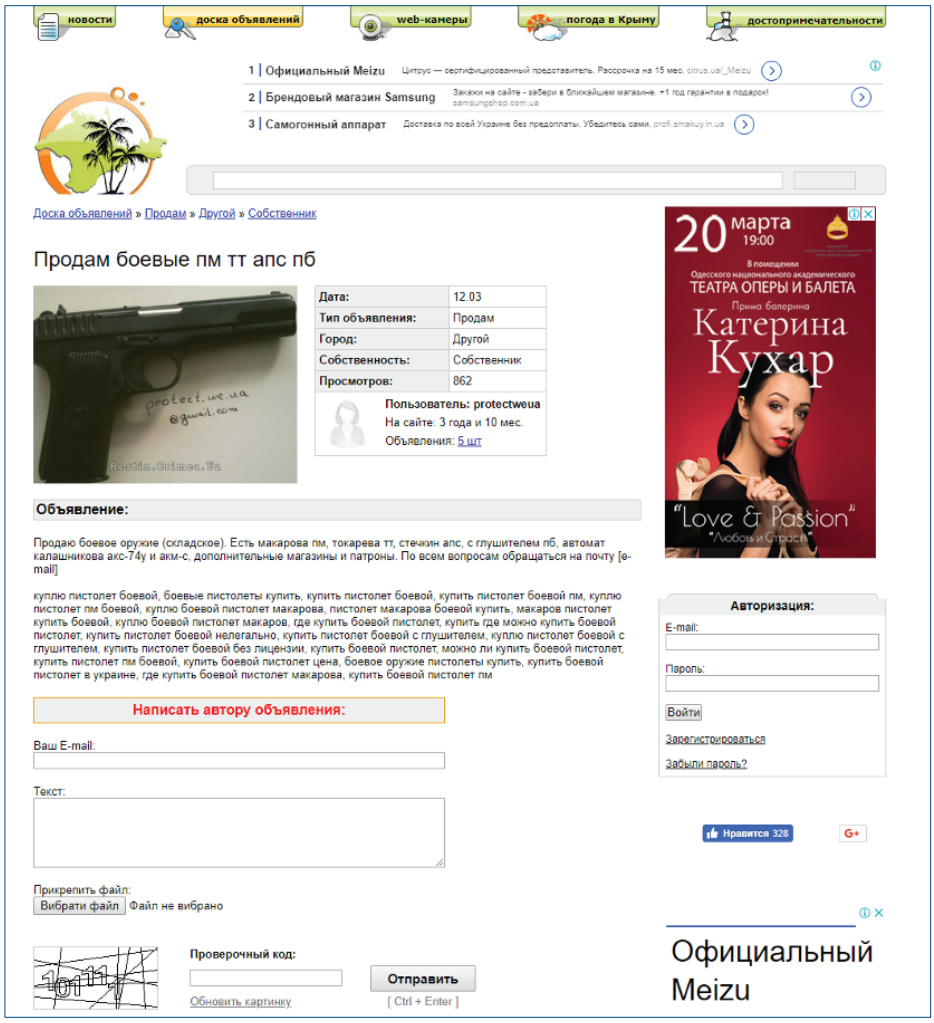






Можна також перейти на вкладку «Завантажити зображення» і відкрити файл, розташований на комп'ютері:

Ввівши звичайний текстовий запит у поле пошуку, можна отримати зображення у результатах. При натисканні на зображення, воно збільшиться та з'явиться посилання для переходу на сайт, на якому розміщено зображення.

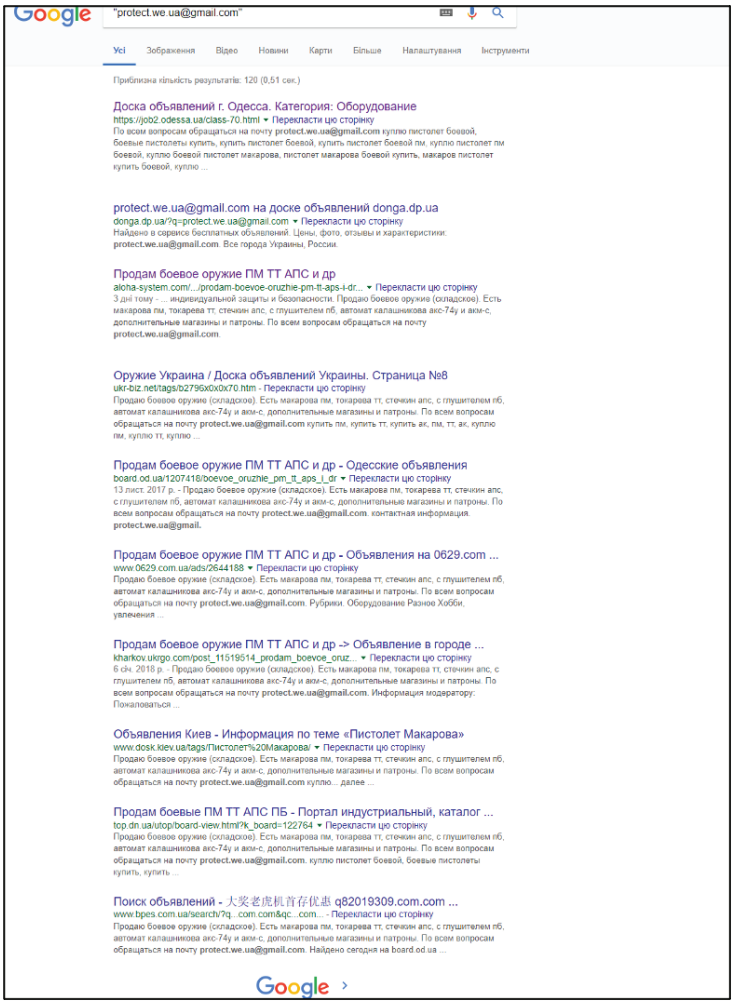


Перейшовши за посиланням, можна потрапити на сайт з розміщеним оголошенням про продаж бойової зброї.

На вибраному фото чітко видно написану від руки адресу електронної пошти. Далі збір інформації слід продовжити в пошуковій системі, аби виявити ресурси на яких вказана ця адреса, акаунти в мережі, з якими вона пов'язана.

Слід зазначити, що запит необхідно вводити із застосуванням лапок «», адже без них Googlebot буде шукати задані слова окремо.

Отримавши результати, можна побачити посилання на майже однакове оголошення на різних сайтах. У ході пошуку інформації на сайті http://ukr-biz[.]net/tags/b2796x0x0x110.htm в одному з оголошень було виявлено номер телефону +3806787**005. Під час пошуку інформації за номером телефону в пошуковій системі нова інформація не виявлена. За цих обставин логічно здійснити пошук сторінки, закріпленої за цим номером у соціальних мережах.



ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-ПОШУКОВОЇ СИСТЕМИ BING

У пошуковій системі Bing налічується лише 6 основних пошукових символів для розширеного пошуку, при цьому символ AND (&) використовується за замовчуванням для всіх запитів. Пошукові оператори системи Bing відображені в таблиці нижче.

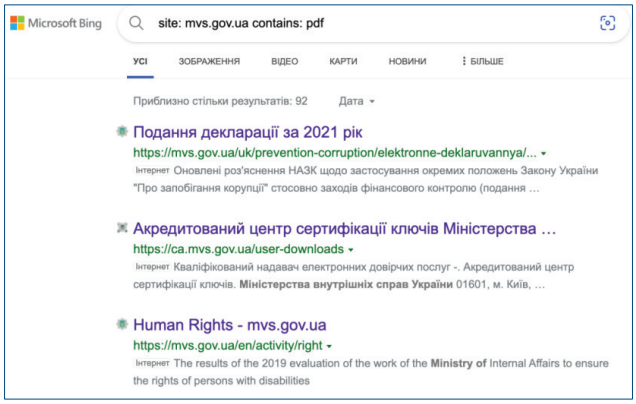
Таблиця 17.2. Пошукові оператори системи Bing

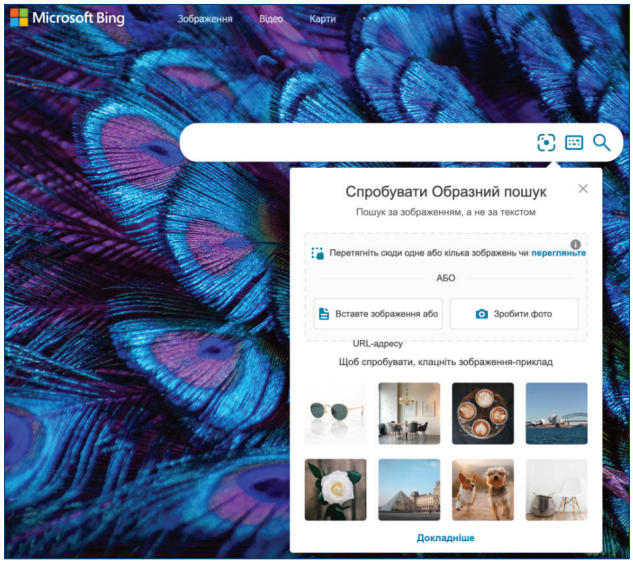
СИМВОЛ	ФУНКЦІЯ
+	Знаходить веб-сторінки, які містять усі терміни перед символом +. Також можна включати терміни, які зазвичай ігноруються.
« «	Знаходить точні слова у фразі.
()	Знаходить або виключає веб-сторінки, які містять групу слів.
AND або &	Знаходить веб-сторінки, які містять усі умови або фрази.
NOT або –	Виключає веб-сторінки, які містять термін або фразу.
OR або |	Знаходить веб-сторінки, які містять будь-яку з умов або фраз.

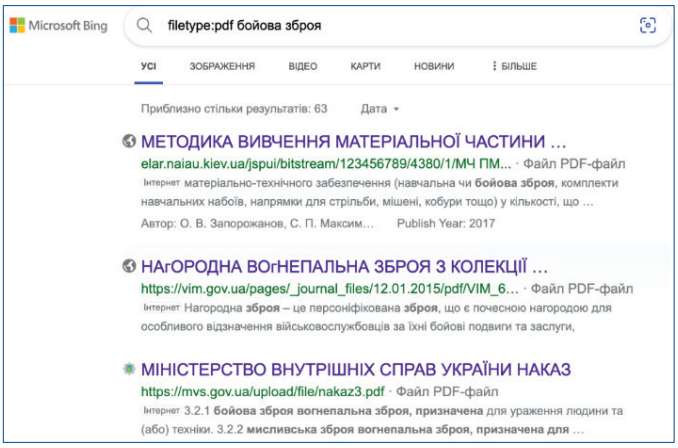
Інші команди, що допоможуть користувачу пошукової системи Bing, наведені нижче.

Команда filetype: дозволяє знаходити файли, які вказуються за допомогою пошукового оператора. Так, якщо потрібно знайти PDF-документ, можна виконати запит наступного виду: filetype:pdf пошукова фраза. Аналогічним чином можна виконувати пошук файлів інших типів.

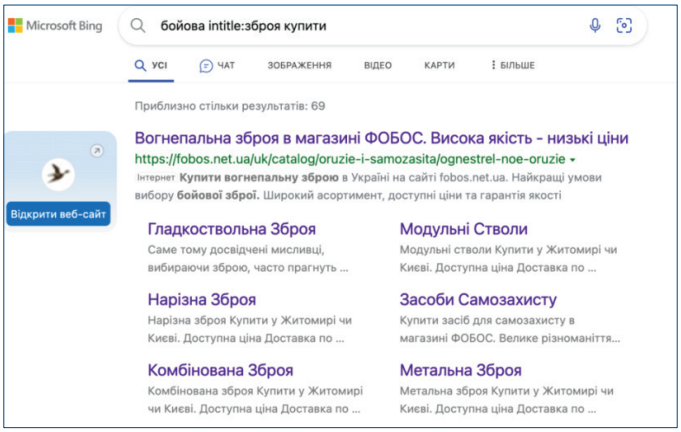
Оператор contains: дозволяє знаходити веб-сторінки, що містять онлайн-документи та мультимедіа файли розшукуваного формату.







Зробити це можна так: site: mvs.gov.ua contains: pdf. Якщо потрібно уточнити результати пошуку, необхідно ввести запит виду ключове слово.



У Bing, як і Google, можна скористатися пошуковими операторами для фільтрації результатів пошуку. Для цього слід використовувати пошукові оператори intitle (пошук за назвою) та inurl (пошук URL). Іншими словами, дані оператори дозволяють знаходити сайти, в title або URL яких міститься ключове слово, яке розшукується.

Пошук по зображенню здійснюється за допомогою натисканням на відповідну піктограму та завантаженням файлу з комп'ютера.

ІНСТРУМЕНТИ АНАЛІЗУ ТА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Засоби кіберзахисту – це різноманітні інструменти, методи та процедури, які використовують для захисту комп'ютерів, мереж, даних та інших інформаційних ресурсів від кіберзагроз.

Розглянемо найбільш розширені інструменти кіберзахисту:

Антивірусні програми. *Програми, які виявляють, блокують та видаляють шкідливі програми, віруси та загрози, які можуть завдати шкоди комп'ютерам та даним.*

Файрволи. *Засоби захисту мережі, які контролюють трафік мережі та блокують небажані підключення та викликано шкідливі програми.*

Мультифакторна аутентифікація (MFA). *Системи, які вимагають від користувачів надання додаткових даних для підтвердження особистості, крім звичайного пароля (наприклад, SMS-код, датчик відбитків пальців тощо).*

Шифрування даних. *Захист інформації шляхом перетворення її в такий формат, який може бути розшифрований тільки за допомогою спеціального ключа.*

Інтранет та екстранет. *Забезпечення захищеного доступу до мережі для внутрішніх і зовнішніх користувачів, що дозволяє контролювати доступ до конфіденційних даних.*

Планування кіберзахисту. *Розробка та впровадження стратегій та планів для попередження, виявлення та реагування на якісь кіберзагрози.*

Аудит безпеки. *Перевірка та оцінка безпеки комп'ютерних систем, мереж та процесів для виявлення слабких місць та підвищення рівня захисту.*

Онлайн-антивірусні програми

Антивірусні програми призначені для захисту комп'ютерів, мобільних пристроїв та інших пристроїв від шкідливих програм, вірусів, троянів, руткитів та іншого шкідливого програмного забезпечення. Вони мають різні характеристики та особливості, але загальна мета забезпечує – безпеку та захист від цих загроз.

В даному підрозділі особливу увагу приділено інструментам, які забезпечують сканування в реальному часі.

Ресурс **Virustotal** аналізує підозрілі файли, домени, IP-адреси та URL-адреси, щоб виявити зловмисне програмне забезпечення та інші порушення, автоматично надсилаючи їх спільноті безпеки.



Ресурс **Esetnod32** є інструментом для простого та ефективного видалення шкідливих програм з будь-якого комп'ютера без встановлення антивірусного програмного забезпечення:

- *сканує без встановлення програми;*
- *виявляє всі типи загроз;*
- *усуває будь-які шкідливі програми, у тому числі з реєстру;*
- *ресурс є безкоштовним.*

Як що стоїть завдання щодо перевірки сумнівних або невідомих файлів або проведення безпечних тестів для забезпечення безпеки і загрози у віртуальному середовищі перед допуском до основної системи, то необхідно використовувати онлайн-пісочниці (sandbox) – це ізольоване середовище, яке використовується для виконання та тестування небезпечних чи невідомих файлів, програм, веб-сайтів або дій без ризику для основної системи.

Основна функція пісочниці виникає в тому, щоб відокремити шкідливо шкідливий код від залишків системи, щоб уникнути інфікування чи пошкодження комп'ютера. Ось деякі ключові функції онлайн-пісочниці:

ізоляція *- забезпечує ізоляцію виконаного коду від основної операційної системи та інших даних;*

спостереження *- відслідковує і реєструє дії, які застосовуються в пісочниці для подальшого аналізу та виявлення загроз;*

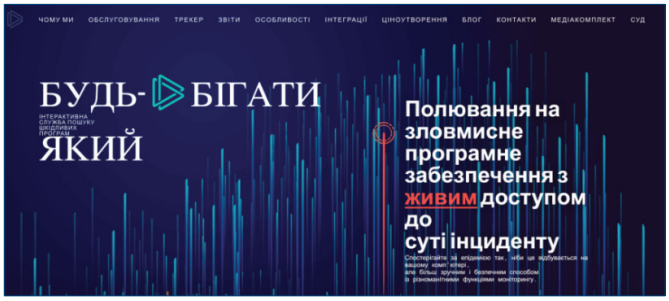
тестування на вразливості *- дозволяє аналізувати код на предмет вразливості та шукати способи атаки;*

тестування мережевих додатків *- використовується для тестування мережевих додатків та служб на вразливості та небезпеки;*

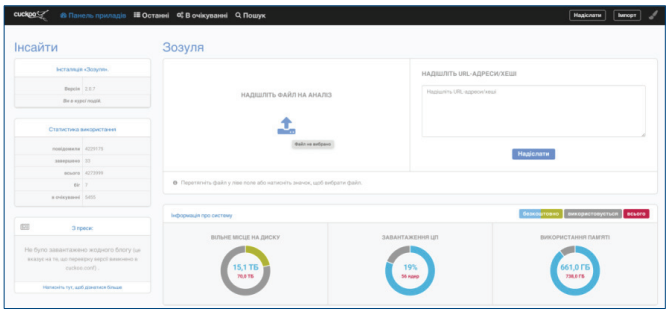
блокування несанкціонованого доступу *- обмежує доступ до ресурсів системи, щоб запобігти несанкціонованому використанню.*

Наведемо наступні робочі приклади:

Ресурс **Any.run** досліджує шкідливе програмне забезпечення. Ресурс надає інтерактивний доступ, досліджує загрози за допомогою фільтра в загальнодоступних матеріалах; динамічно аналізує файли та URL-адреси; відображає кути ATT&CK; надає детальні звіти про шкідливі програми.



Ресурс **Cuckoo.cert** є аналогічним за своїм функціоналом з ресурсом Any.run, але при здійсненні перевірки на декількох ресурсах збільшується відсоток відмовостійкості системи.



Ресурс **Hybrid-Analysis** є безкоштовною службою аналізу шкідливих програм. Аналіз є статичним та динамічним, збагачує робочий процес реагування на інциденти SOC і стек безпеки.

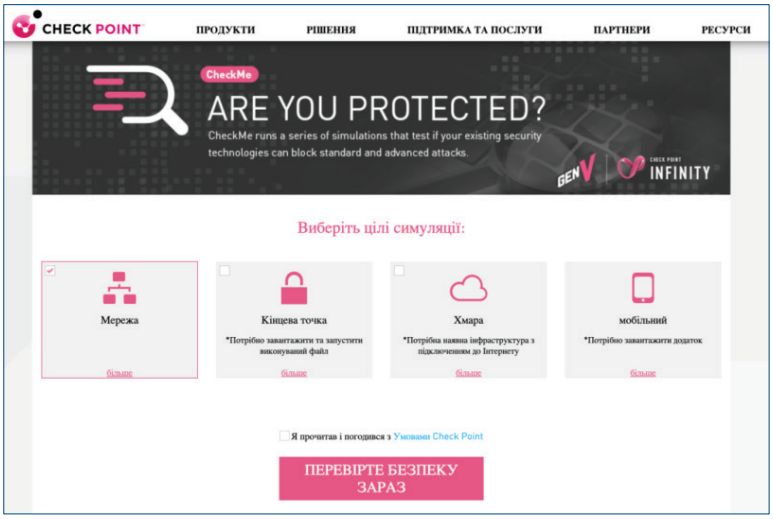


Для отримання додаткової інформації перегляньте сторінку продукту **Falcon Sandbox**. Система аналізу за замовчуванням підтримує будь-який тип PE (.exe, .scr, .pif, .dll, .com, .cpl тощо), Office (.doc, .docx, .ppt, .pps, .pptx, . ppsx, .xls, .xlsx, .rtf, .pub), PDF, APK, виконуваний JAR, компонент сценарію Windows (.sct), ярлик Windows (.lnk), довідка Windows (.chm), програма HTML (.hta) , файл сценарію Windows (*.wsf), Javascript (.js), Visual Basic (*.vbs, *.vbe), Shockwave Flash (.swf), Perl (.pl), Powershell (.ps1, .psd1, . psm1), масштабована векторна графіка (.svg), сценарії Python (.py) і Perl (.pl), виконувані файли Linux ELF, MIME RFC 822 (*.eml), пакети Microsoft Installer (*.msi) і Outlook *.msg файли.

Продукти **Check Point** забезпечують наскрізну безпеку від підприємства до хмари та персональних пристроїв мобільних працівників. Забезпечує:

- безпеку мережі (гібридний центр обробки даних; безпека SD-WAN; безпека без довіри; безпека Інтернету мов).

- хмарну безпеку (полювання на хмарні загрози; безпека без сервера; безпека кон-



тейнерів; безпека AWS; безпека Azure; безпека Google Cloud Platform; відповідність хмарі; DevSecOps; безпека приватної хмари).

- безпеку користувачів та доступу (Secure Access Service Edge (SASE); безпека кінцевої точки; мобільна безпека; безпека електронної пошти).

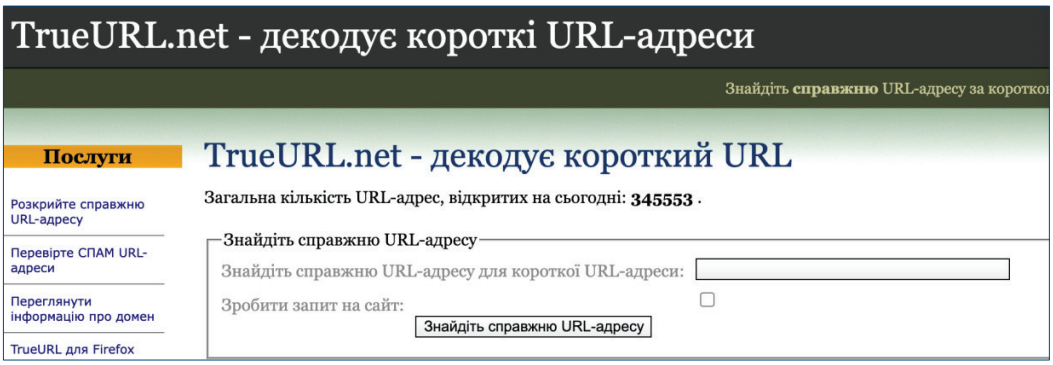
- уніфіковане управління та операції безпеки (кероване виявлення та реагування; розширене виявлення та реагування; управління подіями).

На сьогодні неаби-якої актуальності набуло питання проведення аналізу URL посилання невідкриваючи останню, так як часто зловмисники маскують справжнє посилання. Тому необхідно користуватися наступними ресусами:

Scanurl – безкоштовний ресурс для перевірки веб-сайту/URL на наявність фішингу, зловмисного програмного забезпечення, вірусів, підозрілої поведінки та поганої репутації. Використовується для безечного отримання інформації про URL сайту.



TrueURL – багатофункціональний сервіс, який:
- *декодує коротке URL посилання (надає справжний URL посилання);*
- *надає інформацію про домен сайту.*



Аналізу веб-ресурсів за допомогою WHOIS.

Для аналізу веб-ресурсів використовується **whois** – *це протокол та інструмент для отримання інформації про власників доменів, IP-адреси та інші ресурси в мережі*. Зазначимо, що інформація може різнитися у зв'язку з реєстратором та типом домену.

Основна інформація, яку можна отримати через WHOIS, включає:

Ім'я домену. *Основна частина запиту, яка вказує на конкретний домен, про який необхідно отримати інформацію.*

IP-адреса. *Це числовий ідентифікатор, який призначається конкретному забезпеченню або ресурсу в мережі Інтернет.*

Інформація про реєстранта. *Ім'я та контактна інформація власника домену.*

Інформація про адміністратора. *Ім'я та контактні дані особи, відповідальної за адміністрування домену.*

Інформація про технічний контакт. *Ім'я та контактні дані особи, відповідальної за технічні аспекти домену.*

Інформація про ім'я сервера. *Список імен серверів, які створені для домену.*

Дата реєстрації та термін дії. *Інформація про дату реєстрації домену та термін його дії.*

Інша технічна інформація. *Технічні характеристики домену, такий як статус, DNSSEC тощо.*

WHOIS-інформація корисна для різних цілей, таких як вирішення технічних проблем, визначення власника або контактів для домену, а також для виявлення можливих загроз чи шахрайських дій в

Інтернеті. Важливо відзначити, що деякі домени або реєстри можуть обмежувати доступ до певної інформації із збереженням конфіденційності власників.

Ресурси для отримання WHOIS інформації

myip **synapsint** **torwhois** **whoisology** **ip-geolocation** **2ip**

Ресурси перевірки анонімності

Також для забезпечення безпеки при використанні VPN необхідно користуватися ресурсами перевірки анонімності, які забезпечують перевірку наскільки ви анонімні в мережі, на скільки дані, що надаються вашим комп'ютером/браузером, збігаються з даними, що надаються вашою ip-адресою. Наведемо декілька прикладів ресурсів для перевірки анонімності:

proiptest **cpcheckme** **proxy6** **browsercheck**

Під час проведення моніторингу мережі Інтернет неохідною буває реєстрація на відповідних ресурсах, які мають сумнівну репутаюцію або за правилами проведення розвідки в мережі заборонено користуватися особистими поштовими скриньками, номерами телефону та іншою персональною інформацією. А так як створювати спеціально під конкретне завдання електрону пошту довго, крім того, на неї буде з високим ступенем ймовірності приходити спам-повідомлення, тому необхідно користуватися наведеними нижче ресурсами, які надають можливість відправити та/або отримати одноразовий лист.

temp-mail **tempmailo** **cryptogmail** **anonymousemail** **guerrillamail**

Функціонал типових одноразових поштових сервісів:

- *можливість отримати тимчасову поштову адресу в один клік;*
- *відсутність процесу реєстрації та вимог вказати будь-яку особисту інформацію;*
- *можливість створити скільки завгодно нових адрес;*
- *всі отримані листи зберігаються у тимчасовому сховищі до моменту прочитання їх власником тимчасової скриньки;*
- *автоматичне створення поштової адреси та наявність можливості її змінювати.*

Для забезпечення надійної безпеки в інформаційному просторі необхідно користуватися сервісами, наприклад **DNS Checker**, який надає можливість отримати достовірну інформацію завдяки наступним інструментам:

Інструменти DNS. Вирішують проблеми щодо записів DNS (системи доменних імен) веб-сайту, які допомагають отримувати вхідні запити та направляти їх на правильний сервер, що допомагає серверу отримувати ці запити та відповідати відповідним чином.

- *перевірка IPv4-адреси онлайн. Надсилає пакети ICMP, щоб перевірити IP-адресу призначення або домен, щоб перевірити, чи доступний він у мережі IP;*
- *перевірка пінг IPv6. Перевіряє певне ім'я хоста (домен або IP));*
- *перевірка IP (перевіряє IP-адресу, геолокацію, Інтернет-провайдера, браузер, операційну систему та інше);*
- *traceroute онлайн. Записує весь шлях, через який мережевий запит спрямовується до наданого домену чи IP-адреси;*
- *аналізатор заголовків електронної пошти. Аналізує заголовки електронної пошти та відстежує IP-адресу відправника електронної пошти та IP-адресу Whois;*

- *перевірка чорного списку IP-адрес і електронної пошти. Інструмент визначає, чи домен, IP-адреса чи адреса електронної пошти занесено до DNSBL та інших чорних списків баз даних щодо підозрілої діяльності;*

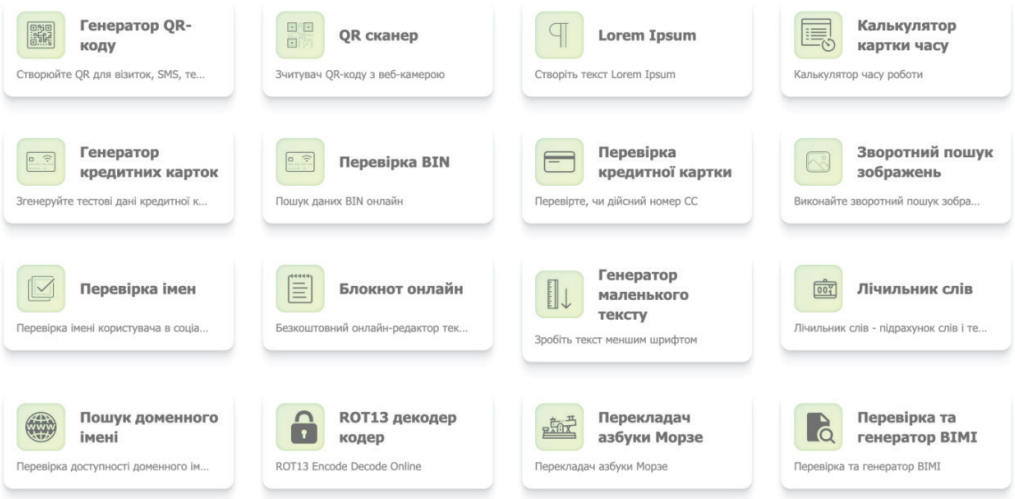
Мережеві інструменти. Мережеві інструменти надають послуги, пов'язані з мережею, і ці послуги можуть включати перевірку відкритих портів, тобто сканування портів TCP і UDP і пошук OUI, тобто перевірку постачальників будь-якого пристрою за допомогою його MAC-адреси або пошуку номера AS, який надає повну інформацію про будь-який номер ASN:

- *онлайн перевірка портів. Перевіряє доступність портів, пов'язаних із певним доменом чи IP-адресою, а також наявність відкритих портів і налаштування переадресації портів на маршрутизаторі;*
- *пошук MAC-адреси. Надає інформацію про MAC-адреси для мережевих карт, встановлених на комп'ютері чи інших пристроях. Надає інформацію, пов'язану з адресою контролю доступу до медіа пристрою, включаючи назву компанії-виробника та країну;*
- *онлайн-генератор MAC-адрес;*
- *пошук ASN. Інструмент ASN Lookup повідомляє деталі ASN WHOIS. Отримується інформація про компанію, яка використовує цей ASN і яке походження цієї компанії (країна, місто, регіон, широта, довгота тощо).*

Інструменти кібербезпеки. Інструменти кібербезпеки призначені для забезпечення безпеки веб-сайтів і відповідності міжнародним стандартам безпеки. Містять інструменти для перевірки безпеки веб-сайту та виявлення будь-яких уразливостей на сайті:

- *перевірка SSL. Засіб перевірки SSL отримує всю можливу інформацію про сертифікат SSL відповідного хосту або домену;*
- *утиліта шифрування паролів. Допомагає шифрувати паролі за допомогою стандартних алгоритмів шифрування. Використовувані алгоритми є двостороннім шифруванням, що означає, що їх можна декодувати пізніше за допомогою того самого алгоритму. Паролі, зашифровані за допомогою цієї утиліти, корисні для зберігання в базах даних тощо;*
- *генератор випадкових паролів. Створює найбільш безпечні короткі та довгі паролі, які не підлягають злому;*
- *перевірка паролів. Вимірює надійність пароля, що використовується.*

Інструменти продуктивності. Призначені для оптимізації робочих процесів (генерація чи сканування QR-кодів, замітки, пошук по фото, робота з текстовою інформацією тощо).



Аналогічним інструменту DNS Checker є ресурс **Weborion**

Цікавим є ресурс перевірки конфіденційності веб-сайтів у реальному часі **Themarkup**, за допомогою якого можна просканувати сайт та отримати звіт, який буде містити наступну інормацію:

- *наявність трекерів реклами;*
- *наявність файлів cookie третіх сторін. Використовуються компаніями з відстеження реклами, щоб створити профіль клієнта на основі використання мережі Інтернет;*
- *наявність відстеження, яке обходить блокувальники файлів cookie;*

- *наявність запису сеансу на веб-сайті. Відстеження руху миші користувача, клацання, натискання, прокручування (так звані теплові карти).*
- *наявність на веб-сайті фіксування натискання клавіш. Реєстрація ключів – це коли веб-сайт фіксує текст, який вводиться на веб-сторінці, перш ніж натиснути кнопку «Надіслати».*
- *наявність Facebook Pixel на веб-сайті. Піксель Facebook – це фрагмент коду, який надсилає назад у Facebook дані про людей, які відвідують сайт, і дозволяє оператору сайту згодом націлити на них рекламу на Facebook.*
- *наявність функції «ремаркетингових аудиторій» Google Analytics. Дозволяє відстежувати користувачів для цільової реклами в Інтернеті. Ця функція дозволяє веб-сайту створювати спеціальні аудиторії на основі того, як користувач взаємодіє з цим конкретним сайтом, а потім стежити за цими користувачами в Інтернеті та націлювати на них рекламу на інших сайтах за допомогою Google Ads і Display & Video 360.*

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Інформаційні технології: підруч. / В.Б. Вишня, К.Ю. Ісмайлов, І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков. Дніпро: ДДУВС, 2021. 492 с.
2. Ісмайлов К.Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації. *Південноукраїнський правничий часопис.* 2016. № 2. С. 110-113.
3. Пошукова система. URL: https://uk.wikipedia.org/wiki/Пошукова_система
4. База даних. URL: https://uk.wikipedia.org/wiki/База_даних
5. Bing. Retrieved from https://uk.wikipedia.org/wiki/Bing
6. DuckDuckGo. URL: https://uk.wikipedia.org/wiki/DuckDuckGo
7. Додаткові параметри пошуку. URL: https://support.microsoft.com/uk-ua/topic/додаткові-параметри-пошуку-b92e25f1-0085-4271-bdf9-14aaea720930
8. Соціальна мережа. URL: http://igroup.com.ua/seo-articles/sotsialna-merezha/
9. Facebook. Інструкція для початківців. URL: http://ipress.ua/ljlive/facebook_instruktsiya_dlya_pochatkivtsiv_2326.html
10. Stalkscan. URL: https://stalkscan.com
11. Вконтакті. URL: https://uk.wikipedia.org/wiki/VK_(соцмережа)
12. Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій): Рішення Ради національної безпеки і оборони України. URL: https://zakon.rada.gov.ua/laws/show/n0004525-17
13. Vk.watch. Retrieved from https://vk.watch
14. Ісмайлов К.Ю. Правовий механізм блокування інтернет-ресурсу в Україні. *Стан та удосконалення безпеки інформаційно-телекомунікаційних систем:* Матеріли міжнародної науково-практичної конференції (м. Коблево, 20-23.06.2017 р.). МТУ МП, 2017. С. 35-39.
15. Telegram. Retrieved from https://uk.wikipedia.org/wiki/Telegram
16. Combot.org. Retrieved from https://t.me/comBot
17. Tgstat. Retrieved from https://t.me/Tgstat
18. Stalkface. Retrieved from https://stalkface.com/en
19. Vk.watch. Retrieved from https://vk.watch
20. Searchlikes. Retrieved from http://searchlikes.ru/login
21. Quick_osint. Retrieved from https://t.me/quick_osint_0_bot
22. InfoBaza. Retrieved from https://t.me/InfoBaza
23. ОкоБога. Retrieved from https://t.me/Oko39boga_bot
24. Telesint. Retrieved from https://t.me/telesint_bot
25. Korniienko, M.V., Horoshko, V.V., Gorbanov, I.M., & Ismailov, K.Y. (2021). Función del análisis criminal en modelos modernos de actividad policial. *Cuestiones Políticas*, 39(68), 415-426. Retrieved from https://www.produccioncientificaluz.org/index.php/cuestiones/article/view/35425
26. Навчально-методичні рекомендації щодо застосування програми Proton VPN для анонімного пошуку оперативнозначущої інформації в Інтернеті / К.Ю. Ісмайлов, Сіфоров, В.С. Жогов, О.І. Одеса: ОДУВС, 2019. 14 с.
27. Навчально-методичні рекомендації щодо пошуку оперативнозначущої інформації в мережі Інтернет К.Ю. Ісмайлов, В.С. Жогов, Л.В. Лефтеров. Одеса: ОДУВС, 2019. 28 с.
28. Навчально-методичні рекомендації щодо пошуку оперативнозначущої інформації на електронних носіях / К.Ю. Ісмайлов, В.О. Русавський, Л.В. Лефтеров. Одеса: ОДУВС, 2019. 14 с.
29. Ismailov, K. (2020). To the issue of personal information circulation in the National police databases. Fundamental and applied researches in practice of leading scientific schools, 38 (2). Canada. P. 41-45.

МЕТОДИ, ІНСТРУМЕНТИ ТА ТРЕНДОВІ НОВАЦІЇ КРИМІНАЛЬНОГО АНАЛІЗУ В УКРАЇНІ

DOI: https://doi.org/10.36486/978-966-2310-66-5-18

Щоб перетравлювати знання, потрібно поглинати їх з апетитом.

Анатоль Франс

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

Дмитро Худенко

МІСЦЕ ТА ТЕРМІНОЛОГІЧНИЙ АНАЛІЗ МЕТОДІВ Й ІНСТРУМЕНТІВ В СИСТЕМІ КРИМІНАЛЬНОГО АНАЛІЗУ

Практична потреба у професійному застосуванні методів та інструментів кримінального аналізу обумовлена попитом на сучасну, технологічну, оперативну та спрощену систему забезпечення діяльності підрозділів кримінальної поліції та органів досудового розслідування. Для керівника кримінальної поліції або органу досудового розслідування залучення можливостей підрозділів кримінального аналізу (ПКА), порівняно із порядком залучення оперативної служби чи оперативно-технічних підрозділів, є одним із найбільш доступних у процесуальному плані. Безпосередню правову основу для цього становлять: ст. ст. 71 та 93 КПК України, ч. 1 п. 21, ст. 8 Закону України від 18 лютого 1992 року № 2135-XII «Про оперативно-розшукову діяльність» [1] та відповідні підзаконні нормативно-правові акти.

Окремі та узагальнені результати залучення служби кримінального аналізу періодично стають публічно доступними, що дозволяє їх порівняння. Одними з перших були відомості за 2020 рік, структуру яких можна представити таким чином:

> *- опрацьовано понад 10 тис. запитів на проведення аналітичної розвідки;*
>
> *- узято участь у розслідуванні понад 4 тис. кримінальних проваджень та близько 2 тис. оперативно-розшукових справ;*
>
> *- здійснено інформаційно-аналітичне дослідження понад 67 тис. об'єктів, у тому числі щодо встановлення майже 20 тис. осіб, 31 тис. транспортних засобів, 6,5 тис. фактів перетину державного кордону.*

На рахунку десятки розкритих серійних угонів елітного автотранспорту, умисних убивств, викритих організованих груп наркоторговців. Серед іншого, до результатів служби належить участь у розслідуванні замаху на умисне вбивство депутата Київської ОДА В'ячеслава Соболєва, захоплення терористом заручників із числа пасажирів автобусу в м. Луцьку, встановлення учасників збройного конфлікту в м. Бровари Київської області, а також учасників організованих злочинних груп, які здійснювали підриви банкоматів на території Вінницької, Дніпропетровської, Запорізької та Харківської областей [2, с. 33-36].

В іншій публікації оприлюднено відомості вже за 2022 рік:

> *забезпечено проведення понад 13 тис. аналітичних досліджень, з яких понад 85% склали оперативні аналізи;*
>
> *досліджено понад 350 тис. різних об'єктів, з яких 106 тис. – фізичних осіб, 81 тис. транспортних засобів та 50 тис. інтернет-ресурсів.*

Серед напрямів діяльності служби кримінального аналізу з'явились нові, а саме:

- *аналіз медіаінформації про ознаки злочинної діяльності військовослужбовців рф, колаборантів та інших протиправних елементів,*
- *встановлення можливої причетності громадян рф та країн-сателітів до збройних формувань країни-агресора або диверсійно-розвідувальних груп,*
- *перевірка фактів примусового вивезення російською федерацією дітей з окупованих територій,*
- *протидія проявам колабораціонізму,*
- *участь у пошуку активів високопосадовців рф та політичної еліти рф [3, с. 8-12].*

Як бачимо, 2022 року відбулась активізація діяльності та з'явились нові напрями діяльності. При цьому спостерігалась велика питома вага оперативного аналізу, що може вказувати на поширення реактивного підходу, який обумовлений війною, а також різнорідними запитами у межах оперативно-розшукових справ та кримінальних проваджень. Активізація правоохоронної діяльності суттєво залежить від інституційного розвитку кримінального аналізу, зокрема, від використання широкої низки його методів та інструментів.

Водночас, визначення місця методів та інструментів в системі кримінального аналізу залежить від розуміння того, який зміст вкладати в таку систему. Відомо, що кримінальний аналіз розуміють як напрям галузі юридичної науки, інститут законодавства, навчальну дисципліну або як професійну діяльність. Усе перелічене є різновидом системи.

У кримінальному аналізі, як навчальній дисципліні, ще не склалась традиційна дворівнева (загальна або особлива частина) чи трирівнева структура курсу (загальна, особлива та спеціальна частина), яку можна зустріти при опануванні таких предметів, як, наприклад, оперативно-розшукова діяльність, криміналістика чи кримінальний процес, як найбільш наближених до кримінального аналізу. Зазвичай, місце для вивчення методів кримінального аналізу відведено на початку або в середині навчального курсу з основ кримінального аналізу, а інструментів наприкінці. Крім того, викладання методів кримінального аналізу відбувається при вивченні характеристик проведення кримінального аналізу за окремими видами кримінальних правопорушень чи за іншими проявами або наслідками девіації.

Наразі, дефініцію «система кримінального аналізу Національної поліції України» не визначено національними законодавчими актами. У наукових джерелах зустрічаємо різні за обсягом або за змістом терміни, наприклад, «система кримінального аналізу в правоохоронних органах» [4, с. 220; 5, с. 6] або «інтелектуальна система кримінального аналізу даних» [6].

Втім, на нормативному рівні визначено складові системи кримінального аналізу НПУ, зокрема, те, що згадана система складається з оперативного, тактичного та стратегічного аналізу [7].

З метою належного формування української системи кримінального аналізу доцільно глибоко вивчати досвід та розвиток зарубіжних систем інформаційно-аналітичного забезпечення правоохоронної діяльності. У цьому сенсі, одним із провідних є практика Великої Британії з розбудови національної моделі - National Intelligence Model (NIM), призначенням якої є забезпечення підвищення на основі проактивного підходу рівня організації та виконання завдань з пошуку, обробки, аналізу, перевірки, збереження та інтерпретації інформації про злочинність і пов'язані з нею явища, як з метою розробки і реалізації оптимальних заходів із протидії злочинності загалом, так і для вирішення конкретних завдань досудового розслідування та оперативно-розшукової діяльності у межах проваджень (справ) зокрема.

Основні елементи системи кримінального аналізу НПУ:

- *засоби (інформаційні ресурси чи програмне забезпечення та пристрої, що уможливлюють процеси збирання та/або зберігання великих обсягів даних);*
- *сили (підрозділи кримінальної поліції, їх інспекторський або оперативний склад, уповноважений на проведення кримінального аналізу, слідчі, які мають знання та навички у сфері кримінального аналізу для роботи з даними);*
- *аналітичні методики, дії з інформацією (процеси, порядки або процедури та/або протоколи пошуку, обробки, аналізу, перевірки, збереження та обміну інформацією, уніфіковані інструкції з проведення аналізу інформації);*
- *нормативно-правове регулювання;*
- *звітність та оцінка ефективності;*
- *планування, прийняття рішень, розподіл ресурсів;*
- *науково-методичне, навчальне та просвітницьке забезпечення;*
- *публічна співпраця та правоохоронна взаємодія.*

У такому разі місце для методів буде визначено серед дій з інформацією, а інструментів – серед засобів.

Існує слушна думка відносно застосування методики кримінального аналізу у протидії кіберзлочинам, сутність якої полягає у її прикладному характері [8]. Її сутність цілком можливо поширити на роль та місце методів та інструментів кримінального аналізу та говорити про їх прикладний характер.

Місце методів та інструментів визначають також їх ефективністю та визнанням результату ініціатором або виконавцем дослідження.

Наприклад, у січні 2023 року інтерв'юерам з числа інспекторського складу ПКА запропоновано за десятибальною шкалою оцінити інтенсивність та ефективність використання ними систем роз-

пізнавання обличчя. Оцінювали продукти від Clearview AI, BigDataPeople Artellence, OSINT та два спеціальні ресурси у ЄІС МВС України.

З'ясовано, що абсолютна першість за вказаними двома критеріями належить продукту від Clearview AI. При цьому, 100 % інтерв'юерів підтверджено доцільність одночасного використання декількох систем (від 3 до 5) розпізнавання із метою досягнення ефективного результату.

У балах найбільша інтенсивність використання належить продукту від Clearview AI (9,38 балів), за ним розташувався продукт від BigDataPeople Artellence (9,23), третє місце — OSINT-ресурси (7,88).

На 8,57 ефективним виявився Clearview AI, один із спеціальних ресурсів ЄІС МВС (8,5) та BigDataPeople Artellence (8,26).

Врешті місце, як і успіх, залежить від технологій, якості та актуальності використовуваних даних, компетенцій виконавця, а також від спроможності поліції адаптуватися до змін у злочинному середовищі та своєчасності використання аналітичних продуктів для прийняття обґрунтованих рішень.

Особливої актуальності питання щодо методів, прийомів та інструментів кримінального аналізу набуває у сучасних умовах збройної агресії рф проти України, коли вчиняються воєнні злочини та злочини проти людяності.

Департамент кримінального аналізу розробляє, впроваджує та застосовує нові методи та напрями здійснення кримінального аналізу, спрямовані на підвищення ефективності протидії злочинності [9].

У цьому зв'язку для ПКА вироблено ряд рекомендацій, які містять необхідну інформацію щодо інформаційних ресурсів.

> *Наприклад, рекомендації щодо практичного використання інформаційних ресурсів та спеціалізованого програмного забезпечення (ботів, додатків тощо) під час розшуку за «відкритими даними» активів осіб, причетних до збройної агресії в Україні та вчинення воєнних злочинів, а також встановлення інформації про членів їх сімей, бізнесу, близького оточення тощо [10], методичні рекомендації проведення кримінального аналізу при вчиненні нападів з метою заволодіння чужим майном, вчинених організованими групами, методичні рекомендації проведення кримінального аналізу при вчиненні крадіжки з банкоматів, методичні рекомендації проведення кримінального аналізу за фактами незаконних заволодінь транспортними засобами, методичні рекомендації проведення кримінального аналізу у боротьбі з наркозлочинністю [11]; методичні рекомендації щодо ефективного використання можливостей ІТС ІПНП ППМ «Телефон» [12] тощо.*

Слід додати, що в практичній діяльності зазвичай прийнято використовувати нормативно-правові термінологічні словосполучення, наприклад, «інформаційні ресурси», «програмне забезпечення» (розділи VIII та X [7]) чи «автоматизована інформаційна система оперативного призначення» [13].

Термінологічні апарати поліцейських шкіл кримінального аналізу оперують поняттями – «метод», «прийом» та «інструмент» кримінального аналізу або ж їх синонімами чи пропонують нові терміни та їх визначення. Наприклад, представниками харківської школи кримінального аналізу використано термін «інструментальні засоби», під якими у широкому сенсі розуміють програмні системи або модулі, методики і методології опрацювання інформації. Також представники цієї школи оперують поняттям «аналітичний інструмент», під яким розуміють у відповідному контексті методику, технічний засіб або програмний продукт (чи модуль), за допомогою яких виконується певна аналітична функція (операція) [14, с. 66; 15, с. 49].

Дніпропетровською школою кримінального аналізу вжито термінологію «методи кримінального аналізу» без тлумачення, але методи класифіковано на загальні та спеціальні, деталізовано їх зміст. Зокрема, у зміст загальних методів вкладено ряд методів здійснення аналізу, що проводяться постійно, в незалежності від об'єкта, який вивчається, у зміст спеціальних – методи, що проводяться з використанням специфічних інструментів та за певними напрямами аналізу [16].

ІАСА використано дещо іншу термінологію або методи кримінального розвідувального аналізу. До них віднесено аналіз злочинців-рецидивістів і аналіз жертв, аналіз кримінальної історії, зв'язків, товарних потоків, комунікацій або соціальних мереж [17].

Ми погоджуємось із думкою іноземних колег про те, що є невелика кількість аналітичних методів, які використовуються і широко застосовуються в різних видах кримінального аналізу так часто, що існує необхідність усім аналітикам знати, як і коли їх застосовувати. Мова йде про мозковий штурм, матрицю перехресного впливу, перевірку ключового припущення, індикатори, аналіз конкуруючих гіпотез, метод самокритики та аналіз «А що, якщо…?» [18, с. 36-37].

На нашу думку, з урахуванням вищевикладеного необхідно сформулювати визначення методів, прийомів та інструментів кримінального аналізу, а також розмежувати їх.

Метод кримінального аналізу – це сукупність специфічних технік та конкретних інструментів, практичне, раціональне та послідовне застосування яких особою, уповноваженою на проведення кримінального аналізу, потенційно та/або реально здатне забезпечити ефективний збір, обробку та дослідження інформації задля систематичного створення аналітичного продукту.

Прийом кримінального аналізу – це специфічна дія особи, уповноваженої на проведення кримінального аналізу, з інструментом, спрямована на досягнення визначеної мети, в ході якої застосовуються інструменти.

Інструмент кримінального аналізу – це інтелект особи, уповноваженої на проведення кримінального аналізу, фізичний прилад або програмний засіб, який застосовано під час виконання прийомів у межах методів.

Методи, прийоми та інструменти слід відрізняти від методології та методики кримінального аналізу. Різниця полягає в обсязі змісту цих понять, їх функціях та призначенні. Якщо розглядати це питання ієрархічно, то методологію, методику, методи, прийом та інструмент слід віднести до різних рівнів прийняття рішень та дій, де методологія визначає найбільш загальне або підхід, методика керує застосуванням методів, методи втілюють через конкретні прийоми, а прийоми реалізуються за допомогою різних інструментів.

Іншими словами

> ***методологією*** *кримінального аналізу визначено загальний підхід до проведення аналітичних досліджень у сфері кримінальної юстиції, їх філософію. Нею окреслено загальноприйняті принципи, підходи та теоретичні межі, які використовують для девіації та пов'язаних із нею феноменів.*
>
> ***Методика*** *кримінального аналізу - це система практичних інструкцій, правил чи процедур, якою визначено, якими методами проводити аналітичні дослідження ознак кримінальних сутностей серед однорідних суспільних відносин, що перебувають під охороною КК України. Саме вона надає конкретні інструкції для виконання завдань дослідження.*

Зазначимо, що на практиці кримінальний аналіз більше розглядають, як інструмент для досягнення цілей оперативно-розшукової діяльності, досудового розслідування та управління в сфері правопорядку. А його інструменти як сучасну технологію [4, с. 218]. Хоча філософія ILP робить акцент на тому, що кримінальний аналіз через свої продукти допомагає керівникам прийняти ефективне рішення у масштабі більшому ніж конкретне провадження або справа.

ПРИНЦИПИ ЗАСТОСУВАННЯ МЕТОДІВ ТА ІНСТРУМЕНТІВ КРИМІНАЛЬНОГО АНАЛІЗУ

Сукупність існуючого потенціалу наукових розвідок у галузі адміністративного, інформаційного права, кримінального права та процесу, криміналістики, кримінології, оперативно-розшукової діяльності, теорії державного управління, а також технік та інструментів, запозичених із журналістики та інформаційних технологій, сприяла розвитку науково-методологічних засад кримінального аналізу, у т.ч. принципів застосування його методів та інструментів. Корисним виявився іноземний досвід і допомога США та ЄС у проєктах US Department of Justice/International Criminal Investigative Training Assistance Program і Право-2 відповідно.

Суттєвий вплив на формування сучасних принципів застосування методів та інструментів кримінального аналізу мав глобальний політичний процес, який розпочався 2015 року, - реформування МВС України. В цей період новоствореною поліцією приділено особливу увагу провідному стратегічному та методологічному підходу, відібраному з п'яти відомих у світі моделей поліцейської роботи [19, с. 48], і розпочато активне запровадження нової філософії концепції діяльності - ILP.

Актуальним лишається впровадження фундаментальних принципів ILP [20, с. 57] із метою забезпечення відповідності міжнародним стандартам з прав людини, захисту персональних даних й уникнення негативного впливу на їх дотримання. Саме ці принципи поряд із конституційними принципами, принципами оперативно-розшукової діяльності та досудового розслідування розглядаються в основі застосування методів та інструментів кримінального аналізу.

Вжиті МВС України та НПУ заходи, у т.ч. із підготовки особового складу, уповноваженого на проведення кримінального аналізу, організації та проведення тематичних конференцій, співпраця з EUAM Ukraine, Europol, IACA, UNOPS, створення центру кримінального аналізу та науково-дослідної лабораторії з проблемних питань кримінального аналізу на базі закладів вищої освіти із специфічними умовами навчання, дозволили отримати унікальний поліцейський досвід із вироблення та застосування методів та інструментів кримінального аналізу.

Утворились дніпропетровська, донецька, київська, львівська, луганська, одеська та харківська поліцейські школи кримінального аналізу. Вперше питанню кримінального аналізу приділено один із підрозділів монографічного дослідження (Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання, Благута Р.І., Мовчан А.В., 2020 р. [4]). У дисертаціях іноді можна відшукати фрагменти у підрозділах, де йде мова про методи та інструменти кримінального аналізу (Ковальова О.В., розділ 2.2. «Правові та організаційні засади застосування засобів інформаційного забезпечення досудового розслідування» [21]).

Жодної дисертації, яка безпосередньо стосується та могла б слугувати однією із перших комплексних праць з проблем кримінального аналізу в поліції, не захищено у спеціалізованих вчених радах. Однак, наразі готується дисертація на тему: «Застосування Національною поліцією кримінального аналізу в протидії незаконному обігу наркотичних засобів, психотропних речовин або їх аналогів в Україні» (Д. Овсянюк, НАВС).

У наукових колах, серед правоохоронців та експертів продовжено дискусії [5; 22; 23; 24] щодо загальновизнаної термінології, стандартів та національних відповідників, а також триває вивчення інших феноменів, пов'язаних із методами та інструментами кримінального аналізу, принципами їх застосування.

Спеціальні академічні та довідкові джерела у власних контекстах містять знання про принципи, які можна розглядати у якості універсальних керівних настанов при застосуванні методів та інструментів кримінального аналізу. Їх авторами вжито спеціальну термінологію. Наприклад, принципи тактичного кримінального аналізу [18, с. 164-188], фундаментальні принципи впровадження ILP, принципи розвідувальної аналітичної діяльності [20, с. 57-59, 62-63], принцип верифікації [25, с. 7-8], принципи управління інформацією, принципи для складання аналітичного звіту, загальні принципи кримінально-аналітичної діяльності або принципи аналітичної діяльності [26, с. 28-29, 48, 52-53, 82] чи принципи письмового звіту [16, с. 115-127] тощо.

На законодавчому рівні відсутнє визначення принципів застосування методів та інструментів кримінального аналізу, що пов'язано із невизначеністю ролі та місця особи, уповноваженої на проведення кримінального аналізу, зокрема, та кримінального аналізу в цілому. Це питання можливо розв'язати нормативно-правовим актом у сфері кримінального аналізу. На нормативному рівні ПКА рекомендовано дотримуватись кримінально-правових засад організації участі осіб, уповноважених на проведення кримінального аналізу у проведені слідчих (розшукових) дій, як спеціаліста (розділ VI Методичних рекомендацій [7]).

Як бачимо, питання про дослідження та формулювання принципів застосування методів та інструментів кримінального аналізу у вітчизняній науці висвітлено фрагментарно та не однозначно.

Термін «принцип» у залежності від контексту може мати декілька основних значень, як-то ключове правило або фундаментальна основа, етична або моральна норма, науковий закон або правило, початок або відправна точка міркувань чи особисте переконання.

На нашу думку,

> *принципи застосування методів та інструментів кримінального аналізу – це спеціальний різновид принципів кримінального аналізу, сутність яких полягає у забезпечені раціональної техніки організації та проведення кримінального аналізу у реалізації проактивного та реактивного підходу до прийняття рішень з протидії злочинності.*

У сучасному кримінальному аналізі принципи застосування методів та засобів відбивають фундаментальні ідеї, що формують техніку та практику дій в цій сфері, яка необхідна для поступового досягнення в першу чергу проакивного прийняття рішень на підставі продуктів аналізу, а вже потім реактивного реагування щодо протидії злочинності та її негативним проявам. Принципи застосування методів та засобів кримінального аналізу є основою для розуміння цього виду діяльності і визначають межі для обраного особою, уповноваженою на проведення кримінального аналізу, підходу у застосуванні науково обґрунтованих методик. Їх значення полягає у створенні ефективної та раціональної системи здійснення кримінального аналізу.

Звісно, якщо розглядати кримінальний аналіз, як міждисциплінарний науковий напрям, то можемо допускати, що також можна керуватися принципами адміністративного, інформаційного права, кримінального права та процесу, криміналістики, кримінології, оперативно-розшукової діяльності, теорії державного управління та інших суміжних галузей знань. Аналогічне твердження буде вірним і на практиці залежно від часу, місця, ролі та характеру аналітичного дослідження, а також його призначення.

Ми вважаємо, що наразі кримінальний аналіз ефективно зарекомендував себе саме у реалізації реактивного підходу правоохоронної діяльності. Його успішно застосовують у комплексі з мож-

ливостями оперативної та оперативно-технічної служби кримінальної поліції. Існують приклади спроб реалізації реактивного підходу [26]. У випадку збільшення питомої ваги прикладів реалізації проактивного підходу в діяльності поліції, особливо у частині SOCTA, стане за можливе говорити про наступальність саме даного підходу, як основного у філософії ILP. У такому разі буде доцільним розглядати його, як засіб забезпечення надання поліцейських послуг населенню.

Зауважимо, що за обсягом термін «*принципи застосування методів та засобів кримінального аналізу*» є меншим аніж, наприклад, «принципи кримінального аналізу», «конституційні принципи» або «принципи оперативно-розшукової діяльності».

Київською та одеською школами кримінального аналізу у контексті імплементації ILP протягом 2016-2019 років першими сформульовано кілька груп принципів або основних положень, зокрема:

1) фундаментальні принципи впровадження ILP (правова, адміністративна та інституційна основа для впровадження діяльності, спрямованої на отримання розвідувальних даних (ILP); законність, необхідність та пропорційність обмежень прав людини; рівність та недискримінація; ефективні засоби правового захисту, нагляд і підзвітність [20, с. 57-59]);

2) принципи розвідувальної аналітичної діяльності (законність, функціональна спеціалізація, розумна достатність, взаємодія, професійна компетентність, об'єктивність, сумісність форм і методів, цілеспрямованість, незалежність, системність, безперервність) [20, с. 62];

3) принципи складання аналітичного звіту (зрозумілість, точність, лаконічність, повнота) [20, с. 82-83];

4) принципи тактичного аналізу:

4.1. психологічні принципи аналізу події [18, с. 118];

4.2. принципи використання методу криміналістичного моніторингу:

4.2.1. основні положення процесу збору криміналістично важливої інформації (законність; системності, цілісність, комплексність, всебічність, об'єктивність, несуперечність, систематичність, конкретність, детермінізм) [18, с. 165-166];

4.2.2. основні положення узагальнення інформації (системності, об'єктивності, несуперечності, систематичності, конкретності) [18, с. 171];

4.2.3. основні положення оцінки якості отриманої інформації (системності, цілісності, комплексності, всебічності, об'єктивності, несуперечності, систематичності, конкретності, детермінізму) [18, с. 173-174];

4.2.4. основні положення систематизації інформації стосовно фактів та обставин певного кримінального правопорушення (системності, цілісності, комплексності, всебічності, об'єктивності, несуперечності, систематичності, конкретності, детермінізму, пріоритетності змісту [18, с. 179];

5) принципи розвідувальної роботи [27, с. 137];

6) принцип верифікації [25, с. 7-8] тощо.

У 2021 році львівською школою кримінального аналізу запропоновано кілька груп принципів саме кримінального аналізу. Їх сутнісна характеристика частково нагадує зміст та назви вищезазначених груп принципів. У науковому обігу з'являється термін «принципи кримінально-аналітичної діяльності», до яких віднесено: законність, функціональна спеціалізація, розумна достатність, взаємодія, професійна компетентність, об'єктивність, сумісність форм і методів, цілеспрямованість, незалежність, системність, безперервність [26, с. 28-29]. Крім того, принципи складання аналітичного звіту доповнено принципом «перевернутої піраміди», який означає винесення висновку на початок звіту. Також, запропоновано групу принципів презентації інформації (точність, лаконічність та повнота) [26, с. 48, 52-53].

Дніпропетровська школа кримінального аналізу (2023) наводить принципи [16, с. 115-127]:

- *письмового звіту (орієнтація на потреби замовника, розташування на першому місці основних висновків з проблемами, формулювання загальної картини проблеми, що розглядається, матеріал має бути структурованим та логічно викладеним, при цьому рекомендовано використовувати чіткі, зрозумілі фрази, намагатися уникати бюрократичного жаргону);*
- *складання якісного письмового звіту (кожна деталь звіту пов'язана з метою його написання, уникнення зайвих слів, намагатися зберігати серйозний тон висловлювання, використовувати дієслова, щоб надати темп переказу, до змісту включені всі аспекти, необхідні для роз'яснення мети, збереження рівноваги, кожен елемент має бути наведено відповідно до його значення).*

На нашу думку, доцільно виокремити ще одну групу принципів - принципи застосування методів та інструментів кримінального аналізу. Для зручності розгляду класифікуємо їх залежно від змісту та характеру, який охоплює правові, етичні, організаційні, методологічні, інноваційні та інші аспекти:

а) принципи правового та етичного характеру:

4. *Верховенства права - жодна людина не є вище права, усі і кожен є рівними перед законом, а застосовувані методи і інструменти кримінального аналізу є засобом справедливості та правопорядку, а не засобом свавілля чи зловживання правом або владою.*
5. *Законність - усі дії з методами, прийомами та інструментами повинні використовуватися виключно в межах чинного законодавства, з повагою до прав і свобод людини та громадянина.*
6. *Етичність – особова, уповноважена на проведення кримінального аналізу, має дотримуватися високих етичних стандартів, включно з конфіденційністю та справедливим ставленням до всіх зацікавлених сторін та об'єктів, які проходять у матеріалах кримінального аналізу.*
7. *Конфіденційність та захист персональних даних - інформація, одержана в результаті застосування методів та інструментів підлягає захисту зберігання та використовується лише в службових цілях із дотриманням правил захисту персональних даних.*
8. *Легальність розробників та походження - відсутність санкцій та ліцензоване використання інструментів та методів кримінального аналізу.*

б) принципи організаційного характеру:

1. *Взаємодії - співпраця із поліцейськими службами та спеціалістами, що задіяні в досудовому розслідуванні.*
2. *Гнучкість та адаптивність – здатність адаптуватися до змінюваних обставин, зокрема, до скорочення або збільшення строків виконання завдань або їх обсягу, і нових викликів кримінального світу або розвитку технологій.*
3. *Зворотній зв'язок - необхідність регулярного аналізу результатів застосування методів та інструментів для коригування тактики і стратегії роботи.*
4. *Інформаційна відкритість – ефективний обмін легалізованою інформацією між різними підрозділами поліції та іншими правоохоронними органами.*
5. *Компетентність – постійне формування професійного ядра особового складу, уповноваженого на проведення кримінального аналізу, здатного ефективно застосовувати сучасні методи та інструменти кримінального аналізу.*
6. *Освіта впродовж служби - організація постійного професійного розвитку співробітників кримінальної поліції для підтримки високого рівня професіоналізму у сфері кримінального аналізу.*
7. *Прозорість - застосування повинно бути відкритим та публічним для громадськості, зрозумілим та обґрунтованим, за винятком випадків, коли це може зашкодити оперативно-розшуковій діяльності або досудовому розслідуванню.*

в) принципи методологічного характеру:

1. *Актуальність - зосередження на актуальній інформації, яка є релевантною для конкретного випадку, застосування методів та інструментів повинно бути спрямовано на дослідження саме відповідної ситуації та відповідного періоду важливості.*
2. *Відтворюваність - дії та результати кримінального аналізу мають бути відтворюваними, щоб можна було перевірити результати та дійти до аналогічних висновків.*
3. *Ефективність - вибір та застосування методів, прийомів і інструментів повинно засновуватися на оцінці їх здатності досягати поставлені цілі з мінімальними витратами ресурсів, а результат має бути у першу чергу ефективним, а вже потім ефектним.*
4. *Інтегративність - застосування не менше 3-5 різних методів та інструментів для багатогранного підходу до виконання завдань.*
5. *Комплексність - поєднання методів та інструментів із різних методологічних підходів та методик для отримання найбільш повного уявлення про сутність дослідження.*
6. *Відповідність – можливість застосування специфічних та потенційно спроможних вирішити завдання методів та інструментів.*
7. *Мультидисциплінарність - використання знань насамперед із суміжних та інших дисциплін, таких як соціологія, культурологія, психологія, інформатика, для глибшого розуміння злочинності та ефективного аналізу її проявів.*
8. *Науковість – всі методи та інструменти повинні базуватися на наукових знаннях і перевірених фактах, а не на необґрунтованих здогадках чи теоріях, мають бути обґрунтованими сучасними досягненнями наукової думки та технологіями, а також досвідом правоохоронної діяльності.*
9. *Об'єктивність - застосування має бути неупередженим, безособовим, виключаючи будь-який вплив особистих симпатій чи антипатій, базуватися на фактах та доказах, розгляді всіх необхідних даних, передбачаючи ретельну оцінку всіх можливих версій і гіпотез.*
10. *Оперативність - своєчасне застосування методів та інструментів для забезпечення негайного реагування на злочинність і мінімізації її наслідків.*
11. *Повноти та всебічності – застосування має охоплювати всю доступну інформацію, враховувати всі факти, обставини і докази без винятку.*
12. *Прогнозування – застосування має допомагати у прогнозуванні злочинної поведінки та ризиків для запобігання кримінальним правопорушенням у майбутньому.*

13. *Ретельність – застосування вимагає детального та ретельного збору, вивчення та оцінки інформації, з увагою до деталей та можливих варіантів розвитку подій.*
14. *Системність – застосування має бути цілеспрямованим, послідовним і структурованим, забезпечуючи логічну послідовність аналітичних дій, використовуючи чітко визначені методики та дії для збору, обробки і інтерпретації даних з метою виявлення зв'язків та взаємозалежностей, а також нових сутностей.*
15. *Стійкість та доступність 24/7 - надійні, витривалі та безперебійно доступні методи та інструменти в будь-який час доби, щоб кримінальна поліція могла ефективно реагувати на виклики сьогодення без затримок.*

г) принципи інноваційного та розвивального характеру:
1. *Інноваційність - пошук та впровадження нових методів та інструментів для постійного покращення функціонування системи кримінального аналізу.*
2. *Тренування – навчання моделей штучного інтелекту.*
3. *Автоматизації – все, що може бути розумно автоматизовано, має бути автоматизовано.*

д) принципи безпосереднього використання інструменту або методу. Розробники або власники інструментів у політиках використання їх програмних продуктів формулюють власне бачення принципів, за умови дотримання яких буде гарантуватись результат. Тому цілком логічним є те, що кожен із методів та інструментів кримінального аналізу має вузько специфічні принципи їх застосування. Принципи або ключові питання, заборони та інші умови користування зазвичай містяться у розділах публічних угод або правил користування ресурсом. наприклад, у політиці конфіденційності, умовах користування, публічній інформації тощо.

Зокрема, сервіс моніторингу реєстраційних даних українських компаній та судового реєстру для захисту від рейдерських захоплень і контролю контрагентів «Opendatabot» рекомендує використовувати його можливості відповідально, у межах чого звертається увага користувача на ряд застережень (*не використовуйте сайт у такий спосіб, що негативно позначиться на нас або на будь-якій третій стороні; не надсилайте небажану або несанкціоновану рекламу, матеріали рекламного характеру чи спам; не завантажуйте програми або інші дані, що є шкідливими або можуть пошкодити сайт тощо*) [28].

Іншим критерієм для класифікації принципів може виступати статус закріплення в офіційних актах (документах): нормативно-правові принципи (матеріальні та процесуальні) або нормативні принципи (організаційно-розпорядчі та політики користування).

ТИПОЛОГІЯ МЕТОДІВ ТА ІНСТРУМЕНТІВ КРИМІНАЛЬНОГО АНАЛІЗУ

Методи кримінального аналізу

Представниками київської та одеської школи кримінального аналізу розкрито зміст значної кількості методів кримінального аналізу незалежно від його виду (аналіз та синтез, порівняння, аналогії, гіпотез, відсотковий, узагальнення, мережі зв'язків, контент-аналіз, спостереження, виключень, пошуку закономірності, класифікацій, моделювання, системний, екстраполяції, ідеалізації, емпатії), які по суті є звичайними методами пізнання, що були запозичені.

Крім того, ними складено перелік із 50 методів, які активно використовуються під час аналітичної діяльності (контрольний лист, приступаючи до роботи, контрольний лист клієнта, переоцінка проблеми, аналіз мережі, ментальні карти, концептуальні карти, операційні карти, сортування, хронології та термінів події, матриці рейтингу, рахунку, пріоритету, SWOT-аналіз, PEST-аналіз, альтернативне прогнозування майбутнього розвитку, плюси-мінуси-недоліки-усунення, виявлення брехні та інші).

Достатньо детально розглянуто методи: картографування аналізу злочину, під яким розуміють процес використання географічної інформаційної системи у поєднані з методами кримінального аналізу, який дає можливість зосередитися на кримінальній або іншій правоохоронній діяльності [18, с. 42]; криміналістичного моніторингу кримінального аналізу - комплексну систему збору, узагальнення, оцінки, систематизації та перевірки криміналістично важливої інформації [18, с.158]; фактологічного аналізу під час досудового розслідування кримінальних правопорушень - спосіб виділення з масиву даних стосовно кримінального правопорушення фактів (або окремих елементів, сегментів, частин фактичних даних) для їх подальшого агрегування (цілісного об'єднання) та встановлення ступеня доказового значення [18, с. 189].

Дніпропетровська школа кримінального аналізу виділяє такі методи кримінального аналізу:

а) загальні - проводяться постійно, в незалежності від об´єкта, який вивчається (аналіз зв'язків, аналіз подій, аналіз процесу або обороту (руху) товарно-матеріальних цінностей (об'єктів), аналіз відомчих джерел, OSINT тощо);

б) спеціальні - проводяться з використанням специфічних інструментів та за певними напрямками аналізу (аналіз комунікативних зв'язків злочинних об'єднань, аналіз телефонних з'єднань, аналіз метаданих, кримінологічна картографія, прогнозування та їх характеристика тощо) [16, с. 40-50].

Представниками львівської школи кримінального аналізу визначено методи залежно від використання їх у оперативному, тактичному та стратегічному аналізі, зокрема:

1. основні аналітичні методи, що використовуються під час проведення оперативного кримінального аналізу (аналіз зв'язків; аналіз соціальних мереж; порівняльний аналіз справи; аналіз інформації з відкритих джерел; складання фінансового профілю; географічне профілювання);
2. аналітичні техніки та методи, що використовуються у тактичному кримінальному аналізі (злочинні моделі (серії); ГІС; статистичний аналіз; аористичний метод);
3. аналітичні техніки та методи у стратегічному аналізі (SWOT-аналіз; PEST-аналіз; SOCTA; аналіз злочинних моделей; аналіз профілів, аналіз тенденцій; аналіз географічного профілювання) [26, с. 5-7].

Крім того, висвітлено ще декілька груп методів кримінального аналізу – оцінки та аналізу ризиків.

Під час аналізу ризиків найпоширенішими вважаються такі методи аналізу ризиків, як мозковий штурм; аналіз конкуруючих гіпотез; огляд статистичних даних; метод Делфі; контрольні листи основних пропозицій; попередній аналіз загроз; індикатори (індекси) ризику; висновки експертів; аналіз сценаріїв; аналіз дерева рішень; причинно-наслідковий аналіз; аналіз дерева подій; аналіз першопричин тощо [26, с. 277-278].

На наш погляд, всі основні види методів кримінального аналізу можна розподілити так:

1) ***кількісні*** *(статистичний аналіз - застосування математичних і статистичних інструментів для вивчення та пізнання сутності числових даних щодо злочинності); кореляційний аналіз (вивчення зв'язків між різними статистичними даними); прогностичний аналіз (використання статистичних методів для прогнозування майбутніх подій на основі поточних та історичних даних);*
2) ***якісні*** *(аналіз сутності змісту - детальне дослідження текстової або мультимедійної інформації для виявлення прихованих змістів і закономірностей); аналіз випадків (глибоке дослідження окремих кримінальних правопорушень або їх серій для розуміння злочинного мотиву та способу); оцінки спеціалістів (використання специфічних знань спеціалістів для інтерпретації даних і виявлення нетипових шаблонів або патернів злочинної діяльності);*
3) ***візуалізації та геопросторові*** *(геоінформаційний аналіз - вивчення географічних даних для виявлення злочинних «теплових точок» та шаблонів (патернів) переміщення злочинців; картографічний аналіз - створення та вивчення шарів наочних карт для візуалізації та розуміння закономірностей або зв'язків у просторі; візуалізація зв'язків (створення мережевих діаграм для зображення зв'язків, візуалізація взаємозв'язків між особами, місцями та подіями; представлення на дашборді чи презентації);*
4) ***хронологічні*** *(часовий аналіз – аналіз даних за часом для виявлення сезонності чи напряму);*
5) ***аналітичні*** *(аналіз зв'язків - вивчення взаємодії чи характеру відношень між особами, групами та об'єктами для виявлення або підтвердження зв'язків; мережевий аналіз - застосування теорії графів для аналізу соціальних та організаційних зв'язків злочинців; профілювання злочинців - аналіз поведінкових шаблонів (патернів), психологічне профілювання; прийоми виявлення шахрайства - аналіз транзакцій, виявлення нестандартних патернів).*
6) ***технологічні*** *- цифрова форензика (вилучення даних з електронних пристроїв, аналіз інтернет-трафіку, логів та ін.), аналіз соціальних мереж (визначення ключових осіб та їх ролей у соціальних мережах; аналіз зв'язків і взаємодій між індивідами або групами);*
7) ***традиційного пізнання*** *(дедукція, індукція, аналіз, синтез, аналогія, наукова абстракція, класифікація, узагальнення, моделювання тощо).*

Згадані види методів не вичерпні, вони поєднуються, їх може бути використано в комплексі для досягнення найбільш повного результату. Поліцейські органи та підрозділи застосовують деякі з цих методів, і під час досудового розслідування конкретного кримінального правопорушення або в оперативно-розшуковий діяльності, і при стратегічному плануванні.

Інструменти кримінального аналізу

У системі кримінального аналізу використовують інструменти для збору, обробки та аналізу даних про злочинність та даних, пов'язаних із злочинністю.

Для зручності представлення пропонуємо інструменти кримінального аналізу класифікувати за такими критеріями:

1. За метою дослідження: попередні (інструменти для першочергового сприйняття та оцінки інформації, а також нормалізації даних); оперативні (для збору та аналізу даних у реальному часі); стратегічні (для довгострокового аналізу та планування).
2. За видом характеру даних: кількісні (статистичні, прогнозування, математичного моделювання); якісні (контент-аналіз, експертні оцінки, аналіз сценаріїв).
3. За методологією аналізу: дескриптивні (картографування злочинності, бази даних злочин-

ності); аналітичні (мережевий аналіз, аналіз шаблонів (патернів)); прогностичні (алгоритми машинного навчання, штучний інтелект).
4. За об'єктом дослідження: для аналізу кримінальних правопорушенн (оцінка ризиків, профілювання злочинців); для аналізу жертв (статистичний аналіз потерпілих, профілювання жертв); для аналізу місць злочину (геопросторовий аналіз, «гарячі точки» злочинності).
5. За способом представлення даних: текстові (рапорти, довідки, доповідні записки, листи); візуальні (карти, графіки, інфографіки); інтерактивні (дашборди, інтерактивні карти, бази даних з можливістю користувацького пошуку).
6. За технологічними можливостями: традиційні (анкети, опитування, інтерв'ю); цифрові інструменти (програмне забезпечення для аналізу даних, онлайн бази даних); інноваційні (Big Data, IoT для збору даних).
7. За сферою застосування: макро-аналіз (розслідування злочинних організацій, злочинів міжнародного характеру); мікро-аналіз: (розслідування конкретних кримінальних правопорушень, локальних подій).
8. За хронологією: для роботи з поточними та архівними даними.

Деякі з цих інструментів можуть бути платними, частково платними або безкоштовними, з відкритим або авторськими правами на код, спеціалізованими і доступні лише для правоохоронних органів чи інших уповноважених осіб, і їх сайти можуть вимагати проходження спеціальної перевірки для доступу.

В одеській школі кримінального аналізу комплексним є підхід до висвітлення класифікації інструментів геоінформаційного характеру для проведення просторового аналізу даних. Їх зміст розкрито її представниками та перелік у контексті тактичного кримінального аналізу [18, с. 89, 106]. До таких інструментів віднесено програмні рішення на різних платформах, різного масштабу та тематичного спрямування, вартості та публічності доступу, як-то ArcGis, EdrawMax, GoogleEarth Pro, Maps.me, SAS.Planet та інші.

Звернута увага на користь таких відомих сервісів, як Bing Maps, DigitalGlobe, eAtlas, Google Earth, Google Maps, Gurtam, iPhone maps, OpenStreetMap, VirtualEarth, Yahoo! Maps, Космоснимки, а також на інформаційні ресурси в Україні, у функціях яких присутні карти злочинності, наприклад, портал CityScale.

Школа львівського кримінального аналізу для виконання завдань стратегічного кримінального аналізу навчає використанню у географічному профілюванні таких інструментів, як ArcGIS, GeoMedia, Global Mapper, GeoDASH, gvSIG, QGIS, MapInfo Pro та IBM i2 iBase (GIS) [4, с. 227-250].

У контексті розкриття змісту інтелектуальних систем прогнозної аналітики правоохоронних органів колективом харківських вчених класифіковано інструментальні аналітичні засоби:
1. Методології і методики аналізу (мережний аналіз, ANACAPA, SOCTA, SWOT-аналіз);
2. Загально використовувані програмні засоби (Microsoft Excel, MatCAD, MatLAB, StatGraph, Statistica, ГІС-истеми та ін.);
3. Традиційні інформаційно-пошукові системи (Ліга-Закон і Google, ІПНП та ін.);
4. Спеціалізовані інформаційно-аналітичні системи і комплекси кримінального аналізу (i2, Palantir, ePOOLICE, PredPol, HOLMS2, RICAS, Maltego та ін.).

При цьому, харківськими вченими зроблено одну з перших спроб визначення особливостей і застосовано компаративістський підхід до аналізу існуючих інструментальних систем для вирішення завдань правоохоронних органів щодо кримінального аналізу [15, с. 49].

Спостерігаємо тенденцію з періодичного створення програмних рішень для потреб кримінального аналізу, про яку свідчить поява таких інструментів від представників київської, луганської та харківської шкіл кримінального аналізу:
- RICAS (Real-time Intelligence crime analytics system) – це інтелектуальна система кримінального аналізу даних, яка включає в себе методи аналітичного пошуку, що є пріоритетним для можливості розкриття злочинів як по гарячих слідах, так і злочинів минулих років [6];
- «Border-v.1.1» - дозволяє здійснити обробку та аналіз інформації з системи «Аркан» Державної прикордонної служби України з метою встановлення фактів одночасного перетину кордону декількома особами шляхом створення готової аналітичної довідки та супровідних матеріалів;
- «Trust-v.1.1» - конвертація витягів Єдиного реєстру довіреностей Міністерства юстиції України з pdf-формату у xlsx (цей формат є складовою частиною табличного процесора MS Excel), що значно розширює можливості правоохоронців щодо аналізу такої інформації та створення аналітичних схем у програмному продукті i2 Analyst's Notebook;
- «Realty-v.1.0», яке дозволяє обробити інформацію з Державного реєстру речових прав на нерухоме майно Міністерства юстиції України шляхом створення окремих файлів csv-формату, у кожному з яких розміщується інформація з Державного реєстру речових прав на нерухоме майно (ДРРП), Реєстру прав власності на нерухоме майно (РПВ), Державного реєстру іпотек (ДРІ), Єдиного реєстру заборон відчуження об'єктів нерухомого майна (ЄРЗВО). Це також

значно розширює можливості правоохоронців щодо аналізу такої інформації та створення аналітичних схем у програмному продукті i2 Analyst's Notebook;
- «Tax-v.1.0», яке здійснює обробку та первинну візуалізації інформації з Єдиного реєстру податкових накладних Державної податкової служби України для встановлення особливостей фінансово-господарської діяльності конкретного платника податків з метою виявлення фактів порушень чинного законодавства [29, с. 191-192];
- Converting audio files into text" - інструмент автоматичного розпізнання аудіо матеріалів у текстовий формат [30].

Перспективними є напрацювання, які можна покласти в основу програмного рішення з методології SOCTA [31], а також розробка В.А. Некрасова у напрямку створення інструменту з ризик-орієнтованого підходу в економічній безпеці.

Унікальним прикладом використання статистичних даних є проєкт від М.В. Карчевського [32], де привертає увагу сама ідея про використання конструктора даних та публічний доступ до нього.

Правоохоронні органи постійно адаптуються до нових технологій, щоб підвищити ефективність кримінального аналізу. В умовах воєнного стану позитивно зарекомендовували себе локальні інформаційні ресурси та он-лайн розробки приватного сектору. Головні секрети цього криються у використані хмарних технологій та доступності. Протягом 2022-2023 років створені нові інформаційні ресурси та сервіси на базі ІПНП - інформаційної підсистеми SOCTA [33], «Воєнний злочинець» [34] та ППМ «Телефон» також виявились корисними та інформативними. Корисними для використання у дослідженнях можуть виявитись ресурси DeepStateMap.Live, де міститься інформація про хронологію та розташування, а також MAXAR, Planet та Sentinel Online , де в зручній формі та на платній або безкоштовній основі представлено різні супутникові знімки нашої планети.

Аналіз публікацій практичних працівників і нормативно-правових документів [2; 13; 35; 36; 37; 38; 39; 40; 41; 42; 43; 44] свідчить про використання можливостей таких інструментів:
- 130 баз та банків даних, створених як у системі НПУ, так і інших центральних і місцевих органів виконавчої влади, підприємств, установ та організацій, серед яких реєстри Державної міграційної служби України, Міністерства юстиції України, Офісу Генерального прокурора. Наприклад, ІТС «ІПНП», АІС ОП МВС України, інформаційно-аналітична система «Облік відомостей про притягнення особи до кримінальної відповідальності та наявності судимості» або обласні та міські програмно-апаратні комплекси типу «Безпечне місто», у т.ч. системи розпізнавання обличчя, зокрема, система розпізнавання облич у міжнародному аеропорту «Бориспіль»;
- аналітичні програмні продукти із використанням технології розпізнавання обличчя, у т.ч. від Artellence Big Data People та Clearview AI;
- програми дослідження операцій із криптоактивами (Chainalysis, Crystal, CipherTrace, DarkOwl, Elliptic, Reactor);
- програми для проведення бізнес-аналізу, вирішення інформаційно-пошукових та аналітичних завдань у сфері безпеки (Страбіс-веб, ORBIS, Ruassets, Youcontrol);
- платформи для проведення розслідувань (DataWalk, Maltego, Profiler, I2, Videris);
- GIS та сервіси надання супутникових знімків (ESRI/ArcGIS, MAXAR);
- системи швидкого перегляду та аналізу записів чи знімків камер спостереження (Video Synopsis);
- сховища даних (Own cloud);
- програмне забезпечення для організації робочого місця та забезпечення аналізу від Microsoft Office, зокрема, Excel, Power BI, Power Point;
- додатки (GetContact, Eyecon та ін.) та різні боти в месенджерах, браузери, розширення до них, а також соціальні мережі.

Успішний кримінальний аналіз часто вимагає поєднання різних інструментів, щоб забезпечити його своєчасність, повноту, глибину та точність. При досліджені операцій з криптоактивами використовували одночасно декілька однорідних програмних рішень – Crystal, CipherTrace, Chainalysis, Elliptic та Reactor.

Слід звернути увагу, що ряд інструментів таких як DataWalk, ORBIS, MAXAR, Profiler, Ruassets, Videris та Youcontrol позитивно зарекомендували під час проведення оперативного та тактичного кримінального аналізу для вирішення завдань з розслідування кримінальних правопорушень, пов'язаних із відмиванням (легалізацією) майна, одержаного злочинним шляхом, і фінансуванням дій збройної агресії на території України [42].

Крім того, історія розвитку органів внутрішніх справ та НПУ говорить про те, що ряд інструментів та інформації не використовується, але вони можуть бути корисними для розкриття кримінальних правопорушень минулих років чи аналізу даних по ТОТ України. Наприклад, до впровадження АРМОР у 2005-2006 роках кожне ГУ (У) МВС(Т) мало різні програмні рішення обліку заяв та повідомлень про кримінальні правопорушення та події, але дані не мігрували до АРМОР. Подібна си-

туація склалась після передачі інформаційно-пошукової системи «Скорпіон» ГУБОЗ МВС України [45] до Департаменту з питань режиму та службової діяльності МВС України матеріальних носіїв інформації, на яких зберігаються дані з цієї системи «Скорпіон». Сформульована пропозиція є неоднозначною і дискусійною, але за умови її належного правового вирішення можливо врегулювання питання подібного роду на майбутнє шляхом внесення змін до законодавства про архівну справу, які б дозволили створювати цифрові архіви та користування ними.

Формування переліку інструментів кримінального аналізу та їх характеристика - завдання досить об'ємне, яке може змінюватись в залежності від конкретних потреб, можливостей та наявних ресурсів поліції, що потребує відповідного бюджетного забезпечення, або підтримки міжнародними партнерами тощо. Водночас, у доповнення до існуючих переліків інструментів кримінального аналізу, що використовуються для різних його аспектів, включно з обробкою даних, аналізом кримінальних правопорушень, візуалізацією даних та іншими функціями, пропонуємо такий перелік:

1. ADF Solutions Digital Evidence Investigator - програмне забезпечення для цифрових розслідувань (https://www.adfsolutions.com)
2. Artellence Big Data People - платформа з унікальним технологіями штучного інтелекту для вирішення OSINT-завдань на основі аналізу великих даних із відкритих джерел (https://artellence.com/)
3. Autopsy - відкритий інструмент для цифрової криміналістики (https://www.autopsy.com)
4. Browser History Examiner - інструмент для аналізу історії веб-браузера (https://www.foxtonforensics.com/browser-history-examiner)
5. Burp Suite - інструмент для тестування безпеки веб-додатків (https://portswigger.net/burp)
6. Celestix HOTPin - рішення для аутентифікації та безпеки (https://www.celestix.com)
7. Cellebrite UFED - рішення для криміналістичного аналізу мобільних пристроїв (https://www.cellebrite.com/en/ufed/)
8. Chainalysis - рішення для аналізу блокчейну (https://https://www.chainalysis.com/)
9. CipherTrace - рішення для аналізу блокчейну (https://ciphertrace.com/)
10. Clearview AI - платформа для розслідувань, яка сприяє розпізнаванню правопорушників (https://www.clearview.ai/)
11. Clearwell Systems (вертикаль Symantec) - інструменти для електронного виявлення та управління інформацією (https://www.symantec.com/clearwell-ediscovery)
12. Crystal Block Explorer - рішення для аналізу блокчейну (https://crystalblockchain.com/)
13. CyberChef - інструмент для аналізу та конвертації даних (https://gchq.github.io/CyberChef/)
14. EnCase Forensic - рішення для цифрової криміналістики та розслідувань (https://www.guidancesoftware.com/encase-forensic)
15. EO Browser - он-лайн платформа, де зібрано архів зображень, отриманих за допомогою супутників Sentinel-1, Sentinel-2, Sentinel-3, Sentinel-5P, архів ЄКА (Landsat 5, 7 та 8), глобальні дані, зібрані Landsat 8-9, Envisat Meris, MODIS, Proba-V та GIBS (https://apps.sentinel-hub.com/)
16. ESRI/ArcGIS - комплекс програмних продуктів для геопросторового аналізу (https://www.esri.com/en-us/arcgis/about-arcgis/overview)
17. Forensic Explorer - програмне забезпечення для забезпечення безпеки даних та розслідувань (http://www.forensicexplorer.com)
18. FTK Imager - інструмент для створення точних копій електронних даних (https://accessdata.com/product-download/ftk-imager-version-4-2-0)
19. Ghiro - автоматизований цифровий зображення аналізатор (http://www.getghiro.org/)
20. Google Earth - це безкоштовна програма компанії Google що відображає віртуальний глобус (https://earth.google.com/)
21. Guidance Software's EnCase eDiscovery - рішення для збору електронних даних без компрометації їх цілісності (https://www.guidancesoftware.com/encase-ediscovery).
22. Hunchly - інструмент, що дозволяє фіксувати цифрові докази при онлайн розслідуваннях (https://www.hunch.ly/)
23. i2 Analyst's Notebook - програма для візуального аналізу зв'язків та мереж (https://i2group.com/i2-analysts-notebook)
24. IDA Pro - дезасемблер та налагоджувач програмного забезпечення (https://www.hex-rays.com/products/ida/)
25. Importgenius - рішення для пошуку глобальних записів імпорту/експорту (https://www.importgenius.com/)
26. Logikcull - хмарний інструмент для управління розслідуваннями і виявленням даних (https://www.logikcull.com)
27. Magnet AXIOM - комплексне рішення для цифрових розслідувань (https://www.magnetforensics.com/products/magnet-axiom/)
28. Maltego - інструмент для збору та аналізу інформації про зв'язки (https://www.maltego.com)
29. Secure Watch MAXAR - інструмент для геопросторової розвідки (https://www.maxar.com/)
30. Metasploit Framework - інструмент для розробки та виконання експлойтів проти віддаленої машини (https://www.metasploit.com)
31. Micro Focus Intella - інструмент для пошуку інформації та криміналістичного аналізу електронних доказів (https://www.microfocus.com/en-us/products/intella/overview)

32. MOBILedit Forensic Express - інструмент для аналізу мобільних телефонів (https://www.mobiledit.com/forensic-express)
33. Nessus - програма для оцінки вразливостей (https://www.tenable.com/products/nessus)
34. NetWitness Suite - платформа для аналізу безпеки мережі (https://www.rsa.com/en-us/products/threat-detection-response)
35. Nuix Investigator - рішення для аналізу, пошуку та управління даними (https://www.nuix.com/products/nuix-investigator)
36. ORBIS - рішення для аналізу, пошуку та управління даними про компанії у всьому світі (https://http://bvdinfo.cn/)
37. OSForensics - виявлення підозрілих файлів та активності на комп'ютерах (https://www.osforensics.com/)
38. Oxygen Forensic Detective - програма для криміналістичного аналізу мобільних пристроїв (https://www.oxygen-forensic.com)
39. Palantir Gotham - платформа для інтеграції, управління та аналізу великих даних (https://www.palantir.com/platforms/gotham/)
40. Paraben's E3 Platform - універсальна платформа для цифрової криміналістики (https://paraben.com/e3-forensic-platform/)
41. Passware Kit Forensic - програма для відновлення паролів та розшифровки даних (https://www.passware.com/kit-forensic/)
42. Power BI - рішення для бізнес-аналітики, націлене на інтерактивну візуалізацію (https://www.microsoft.com/ru-ru/power-platform/products/power-bi?market)
43. ProDiscover Forensic - програма для забезпечення цілісності доказів та проведення розслідувань (http://www.techpathways.com/ProDiscoverDFT.html)
44. QGIS - відкрита система інформації для картографування та аналізу (https://www.qgis.org)
45. Recon Lab - комплексний набір інструментів для аналізу від Sumuri (https://sumuri.com/software/recon-lab/)
46. Relativity - платформа для керування та аналізу юридичних даних (https://www.relativity.com)
47. SAS Visual Analytics - інструмент для візуалізації та аналізу даних великого обсягу (https://www.sas.com/en_us/software/visual-analytics.html)
48. SIFT Workstation - безкоштовний набір інструментів для цифрової криміналістики (https://digital-forensics.sans.org/community/downloads)
49. Snort - система виявлення та запобігання вторгнень (https://www.snort.org)
50. Spector CNE Investigator - інструмент для моніторингу комп'ютерної активності (https://www.veriato.com)
51. Splunk - платформа для аналізу та візуалізації машиногенерованих даних (https://www.splunk.com)
52. Tableau - інструмент для інтерактивної візуалізації даних (https://www.tableau.com)
53. The Sleuth Kit (+Autopsy) - набір інструментів для цифрової криміналістики (http://www.sleuthkit.org)
54. Veriato Investigator - рішення для моніторингу активності користувачів і внутрішніх розслідувань (https://www.veriato.com/products/veriato-investigator)
55. Video Synopsis - рішення для швидкого аналізу відеоматеріалів (https://www.briefcam.com/)
56. WinHex і X-Ways Forensics - редактор шістнадцяткових значень та інструмент для аналізу (https://www.x-ways.net)
57. Wireshark - аналізатор мережевих пакетів (https://www.wireshark.org)
58. X1 Social Discovery - збір даних з соціальних мереж для цифрових розслідувань (https://www.x1.com/products/x1-social-discovery/)
59. X-Ways Forensics - розширений інструмент для цифрової криміналістики (https://www.x-ways.net/forensics/index-m.html)
60. Youcontrol - рішення для комплаєнсу, аналізу ринків, ділової розвідки та розслідувань.(https://youcontrol.com.ua/)

На нашу думку, достатньо складно сформувати універсальний перелік інструментів кримінального аналізу через постійний та випереджувальний їх розвиток. Водночас, об'єктивним є періодичне звернення до експертної думки, а також збірок інструментів [46], оновлених видань [47; 48], спеціалізованих форумів або он-лайн ресурсів від професійних спільнот та розслідувачів з результатами їх досліджень [49; 50; 51].

Наступний перелік інструментів кримінального аналізу можна розглядати у якості систематизованого результату пошуку іноземних термінологічних відповідників:

1. Алгоритми машинного навчання (Machine Learning Algorithms)
2. Аналіз банківських даних (Banking Data Analysis Tools)
3. Аналіз великих даних (Big Data Analytics)
4. Аналіз відео (Video Analysis Tools)
5. Аналіз голосу (Voice Analysis Tools)
6. Аналіз ДНК (DNA Analysis Tools)
7. Аналіз зброї (Ballistics Analysis Tools)
8. Аналіз зв'язків (Link Analysis Tools)
9. Аналіз кіберзлочинності (Cybercrime Analysis Tools)
10. Аналіз мікровиразів обличчя (Micro-Expressions Analysis Tools)

11. Аналіз мовного забезпечення (Linguistic Analysis Tools)
12. Аналіз рукописних текстів (Handwriting Analysis Tools)
13. Аналіз соціальних медіа (Social Media Analysis Tools)
14. Аналіз транзакційних даних (Transactional Data Analysis Tools)
15. Аналітичне обладнання для детектування наркотиків (Drug Detection Analytical Equipment)
16. Аналітичні платформи (Analytical Platforms)
17. Аудіоаналіз (Audio Analysis Tools)
18. Аудіовізуальні засоби для допитів (Audio-Visual Interview Tools)
19. Бази даних відкритих джерел (Open Source Databases)
20. Бази даних з юриспруденції (Legal Research Databases)
21. Бази даних злочинців (Criminal Databases)
22. Бази даних про викрадене майно (Stolen Property Databases)
23. Бази даних про викрадені транспортні засоби (Stolen Vehicle Databases)
24. Біометричні системи (Biometric Systems)
25. Географічні інформаційні системи (GIS)
26. Інструменти для аналізу електронних пристроїв (Electronic Device Analysis Tools)
27. Інструменти для аналізу хмарних сервісів (Cloud Service Analysis Tools)
28. Інструменти для аудиту безпеки (Security Auditing Tools)
29. Інструменти для виявлення шахрайства (Fraud Detection Tools)
30. Інструменти для моделювання злочинності (Crime Modeling Tools)
31. Інтернет речей (IoT) для збору даних
32. Кіберзахист та антивірусні програми (Cybersecurity and Antivirus Software)
33. Автоматизована диспетчерська допомога (Computer-Aided Dispatch - CAD)
34. Криміналістична фотографія (Forensic Photography Equipment)
35. Криміналістичне програмне забезпечення (Forensic Tools)
36. Кримінально-аналітичне програмне забезпечення (Crime Analysis Tools)
37. Мережевий аналіз (Network Analysis)
38. Опитування і анкети (Surveys and Questionnaires)
39. Поліграф (Polygraph Examinatio Equipment)
40. Інструменти з пошуку в базах даних (Database Query Tools)
41. Предиктивна аналітика (Predictive Analytics)
42. Програмне забезпечення для аналізу контенту (Web Content Analysis Tools)
43. Програмне забезпечення для аналізу тексту (Text Analysis Tools)
44. Програмне забезпечення для збору цифрових доказів (Digital Evidence Capturing Tools)
45. Програмне забезпечення для картографування злочинності (Crime Mapping Tools)
46. Симуляційні програми для тренувань (Simulation Training Programs)
47. Система автоматичного визначення місцезнаходження (Automatic Location Identification - ALI)
48. Системи адміністрування доказів (Evidence Management Systems)
49. Системи криміналістичного аналізу мобільних пристроїв (Mobile Forensic Tools)
50. Системи відеоспостереження (Video Surveillance Systems)
51. Системи віртуальної реальності для реконструкції місця злочину (VR Crime Scene Reconstruction)
52. Системи документування місця злочину (Crime Scene Documentation Systems)
53. Системи ідентифікації транспортних засобів (Vehicle Identification Systems)
54. Системи обробки зображень (Image Processing Systems)
55. Системи розпізнавання облич (Facial Recognition Systems)
56. Системи управління кримінальними записами (Records Management Systems - RMS)
57. Системи штучного інтелекту (Artificial Intelligence Systems)
58. Системи ідентифікації за відбитками пальців (Fingerprint Identification Systems)
59. Статистичне програмне забезпечення (SPSS)
60. Фінансовий аналіз (Financial Analysis Tools).

СПІВВІДНОШЕННЯ МЕТОДІВ КРИМІНАЛЬНОГО АНАЛІЗУ З СУМІЖНИМИ ГАЛУЗЯМИ

Система кримінального аналізу потребує мультидисциплінарного підходу. Методи та інструменти кримінального аналізу можуть доповнювати один одного, взаємодіяти та співвідноситися із методами та підходами, що використовуються у різних сферах та галузях, пов'язаних з інформаційними технологіями, кримінальною юстицією та протидією злочинністю, як видами людської діяльності. Основними суміжними галузями діяльності для кримінального аналізу є оперативно-розшукова діяльність, діяльність органів досудового розслідування, галузь криміналістики, кримінології, адміністративного права, теорії державного управління, інформаційних технологій та OSINT.

Наприклад, кримінальний аналіз може бути проведено і у межах оперативно-розшукової справи, і у межах кримінального провадження за наявності відповідних підстав [16, с. 88-104].

Співвідношення можна проілюструвати через такі основні напрями та сфери, галузі або області публічної та приватної діяльності:

Напрями співвідношення методів кримінального аналізу	Сфери або галузі публічної та приватної діяльності							
	Оперативно-розшукова діяльність	Досудове розслідування	Криміналістика	Кримінологія	Адміністративне право	Державне управління	Інформаційні технології	OSINT
Правове регулювання інституту кримінального аналізу	+	+			+	+		
Інформаційне забезпечення кримінального аналізу	+	+	+	+			+	+
Збір або виявлення майбутніх доказів за допомогою кримінального аналізу	+	+	+					
Збір та обробка даних за допомогою кримінального аналізу	+	+			+	+		
Зберігання та управління даними, утвореними внаслідок кримінального аналізу	+				+	+		
Аналіз даних за допомогою кримінального аналізу	+	+			+			
Візуалізація даних	+	+						
Кібербезпека даних, утворених внаслідок кримінального аналізу, або отримуваних для роботи	+		+				+	
Автоматизація та роботизація процесів для потреб кримінального аналізу							+	+
Взаємодоповнення та комплексне використання методів	+	+	+	+	+	+	+	+
Профілювання злочинності за допомогою кримінального аналізу	+	+						
Прийняття рішень на підставі даних кримінального аналізу	+	+			+	+		
Планування діяльності на підставі даних кримінального аналізу	+	+			+	+		
Визначення ресурсів, сил та засобів на підставі кримінального аналізу	+	+			+	+		
Підтримка імперативності					+			
Превенція на підставі результатів кримінального аналізу	+	+		+	+	+	+	

КЛЮЧОВІ ТЕНДЕНЦІЇ РОЗВИТКУ МЕТОДІВ ТА ІНСТРУМЕНТІВ КРИМІНАЛЬНОГО АНАЛІЗУ

Розвиток методів та інструментів кримінального аналізу є важливим складником сучасної правоохоронної діяльності. У світі стрімкого нарощування інформаційних потоків і розвитку технологій кримінальний аналіз стає все більш складним і багатогранним. Розвиток інструментів та методів кримінального аналізу вимагає інтеграції технічних новацій, методологічних підходів, правової бази та висококваліфікованих фахівців, що в сукупності забезпечує ефективне виявлення, попередження та розслідування кримінальних правопорушень.

Розглянемо загальні шляхи розвитку:

1) *технологічний* - біометричні технології у частині розпізнавання обличчя та предметів, відбитків пальців, ДНК-профілювання; цифровий аналіз – використання програмного забезпечення для аналізу цифрових доказів, таких як метадані файлів, логи доступу до систем тощо; штучний інтелект і машинне навчання – для виявлення зразків поведінки, прогнозування злочинності, аналізу текстів і зображень; Big Data аналітика – обробка великих даних для виявлення тенденцій та зв'язків; аналітична платформа або середовище – впровадження єдиного інструменту для проведення аналізу та збереження його результатів; інтероперабельність доступу – отримання доступу до інформаційних ресурсів в межах ЄІС МВС України;

2) *методологічний* - профайлінг - аналіз характеристик злочинців та злочинів для створення «портрета» потенційного правопорушника; кримінальна геоінформація - використання геоінформаційних систем для аналізу місць вчинення злочинів; часовий аналіз - вивчення часових моделей злочинності для розробки стратегій патрулювання і запобігання злочинам;

мережевий аналіз - виявлення зв'язків між особами, організаціями та подіями; розробка термінологічного словника та іноземних відповідників; розроблення методології та техніки кримінального аналізу з попередження, виявлення, розкриття та досудового розслідування різних видів кримінальних правопорушень, а також воєнних злочинів, розшуку осіб, які переховуються від органів кримінальної юстиції, встановлення осіб невпізнаних трупів;

3) *практичні прийоми* - тактичний аналіз - короткостроковий аналіз для негайного реагування на злочини; стратегічний аналіз - довгострокове планування на основі аналізу тенденцій та прогнозування розвитку злочинності; оперативно-розшукові заходи - використання кримінального аналізу для забезпечення розшуку злочинців та напрямку пошуку доказів;

4) *нормативно-правове регулювання* - законодавче забезпечення - розробка та вдосконалення законодавства для регулювання використання нових технологій у кримінальному аналізі; статус особи, яка проводить кримінальний аналіз - внесення змін до державного класифікатора професій;

5) *етика та приватність* - врегулювання питань, пов'язаних із захистом особистих даних і приватності під час кримінальних розслідувань;

6) *навчання, освіта та постійне оновлення знань* - стандартизація освіти з кримінального аналізу; спеціалізовані програми навчання - підготовка фахівців, які можуть ефективно використовувати новітні інструменти та методи; постійне оновлення знань - організація семінарів, тренінгів та роботи над помилками та визначення причин нерозкриття кримінальних правопорушень за гарячими слідами, залучення до наукових конференцій та круглих столів провідних представників приватного сектору; спеціалізовані виставки та змагання; подальше вивчення досвіду Великої Британії, країн ЄС та США).

Перспективи розвитку методів та інструментів кримінального аналізу залежатимуть від безлічі факторів. Прогнозування розвитку може представляти складність через технологічне і соціальне середовище, що швидко змінюється. Але їх можна розглядати у трьох основних напрямах: технологічний розвиток; розвиток методології; зміни в нормативно-правовому полі, а також на короткострокову (5 років), середньострокову (10 років) та довгострокову (20 років) перспективи.

Найбільш ймовірні світові тенденції:

- *короткострокова перспектива (5 років):*
  - ✓ *штучний інтелект та машинне навчання* - швидке удосконалення алгоритмів для аналізу великих даних, включно з реальним часом;
  - ✓ *доповнення реальності та віртуальна реальність* - використання цих технологій для тренування та реконструкції місць подій та виявлення злочинів;
  - ✓ *мобільно-оперативні дослідження* - поліпшення мобільних технологій дозволить проводити швидкі та ефективні на місці дослідження;
  - ✓ *інтероперабельність* - інтеграція через централізований шлюз різних джерел інформації і баз даних для швидкого обміну даними, що покращує комунікацію;
  - ✓ *хмарні технології* – часткова міграція даних у хмарні сервіси, досягнення підвищеної відмовостійкості;
  - ✓ *розслідування воєнних злочинів* – активізація досліджень у сфері воєнних злочинів.

- *середньострокова перспектива (10 років):*
  - ✓ *автоматизація розслідувань* - впровадження повністю автоматизованих систем для рутинних процесів кримінального аналізу;
  - ✓ *предиктивна поліція* - розробка алгоритмів для аналізу ймовірності вчинення злочинів у певних районах;
  - ✓ *біотехнології* - значні вдосконалення в геноміці та аналізі ДНК для швидкої ідентифікації осіб;
  - ✓ *кібербезпека* - розвиток методів аналізу для захисту та розслідування кіберзлочинів.

- *довгострокова перспектива (20 років):*
  - ✓ *квантові комп'ютери* - можливе використання квантових технологій для швидкісного декодування інформації та розкриття зашифрованих даних;
  - ✓ *глобальні системи спостереження* - розвиток супутникових технологій та дронів для всебічного моніторингу;
  - ✓ *нейротехнології* - можливість читання думок та інтенцій через нейроінтерфейси, що можуть знайти застосування в детекції брехні або в розслідуваннях.
  - ✓ *соціальні та етичні зміни* - розвиток нових норм та правил, що регулюватимуть використання провідних технологій, з посиленою чи нейтральною увагою до приватності та прав людини.

Загалом, перспективи розвитку кримінального аналізу є надзвичайно великими і обіцяють значне посилення можливостей правоохоронних органів. Однак, поряд із технологічним прогресом, необхідно враховувати й потенційні ризики, такі як порушення приватності, зловживання повноваженнями та етичні дилеми, що виникають у зв'язку з новими технологіями.

Очікуємо, що ці методи будуть тісно пов'язані з використанням нових технологій, покращенням алгоритмів та аналітики, а також суворим дотримання законодавства та приватності інформації. Суть даного твердження розглянемо за допомогою декількох ілюстрацій.

> *У контексті розвитку технологій кримінального аналізу особливо актуальним стає застосування засобів штучного інтелекту, експрес-аналізу ДНК, фенотипування, а також аналізу емоцій та ризиків за голосом.*

Аналіз нормативно-правового регулювання показав, що за останні три роки в українському законодавстві розпочалася регламентація статусу кримінального аналізу [1; 52; 53; 54]. Поряд із цим у дотичній сфері правотворчості введено в дію новий закон [55], що розбудовує правову базу для обробки геномної інформації людини з метою її державної реєстрації.

І хоча ПКА не є власниками електронної біометричної інформації, але їм не заборонено її законне використання, через що виник досвід роботи з такою інформацією.

Інтерес до цієї теми викликає наша ідея про інтеграцію рішень від провідних світових компаній, включаючи Ande, ClearView AI та Parabon NanoLabs із США, а також Nemesysco Ltd із Ізраїлю. Крім Parabon NanoLabs, що спеціалізується на розробці нанофармацевтичних препаратів та надає послуги фенотипування ДНК для правоохоронних органів, усі компанії отримали значний досвід використання своїх продуктів в Україні після 23 лютого 2022 року.

Для потреб НПУ було поставлено портативні ДНК-лабораторії від компанії Ande – одного з лідерів у технології швидкого визначення ДНК, яку використовують військові та правоохоронні органи. ClearView AI надано одне з найкращих у світі програмних рішень для зіставлення людського обличчя.

У користуванні українських поліцейських також є програмне забезпечення LVA від компанії Nemesysco Ltd, призначене для передового та неінвазивного аналізу голосу для виявлення емоцій та оцінки ризиків [56].

Ми переконані, що успіх застосування вищезазначених технологій полягає у реалізації комплексного підходу. Наприклад, у випадках, коли результати зіставлення осіб або ДНК-профілів відсутні, ключову роль грає фенотипування ДНК [57]. Портрет, отриманий в результаті фенотипування, може бути звірений з національними інформаційними репозиторіями або базою даних ClearView AI, що містить понад 20 млрд зображень з Інтернету, включаючи соціальні мережі.

У 1973 році Національна консультативна комісія зі стандартів і цілей кримінального правосуддя в США виступила з різкою заявою щодо розвідувальної роботи. Комісією закликано усі правоохоронні органи та кожну державу негайно створити та підтримувати спроможність збирати та оцінювати інформацію та поширювати розвіддані таким чином, щоб захищати право кожної людини на приватне життя, одночасно обмежуючи організовану злочинність та забезпечуючи громадський порядок [58, с. 5].

Статтею 19 Конституції України [59] встановлено, що органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах, повноважень та у спосіб, що передбачені Конституцією та законами України.

За останні три роки в Україні спостерігається зростання кількості місць, де встановлені системи відеоспостереження з функцією розпізнавання обличчя. Суспільство проявляє інтерес і до практичного, і до наукового використання технології порівняння біометричних даних особи з різними шаблонами (патернами). На ринку з'являється попит на продукти та послуги, пов'язані з біометричним порівнянням, навіть відомі браузери пропонують безкоштовний пошук зображень. Законодавство ЄС та рекомендації щодо штучного інтелекту та захисту персональних даних періодично оновлюються, що вимагає теоретичного аналізу. Особливо актуальним стало використання цієї технології в умовах воєнного стану через зростання випадків успішного застосування відповідного програмного забезпечення [40].

Для карного розшуку, як однієї із найбільших служб кримінальної поліції, це питання є вкрай актуальним, перед яким завжди гостро поставало розкриття одного із самих найпоширеніших типів кримінальних правопорушень серед територіальних громад - неочевидних або «фактових» злочинів, учинених «в умовах вулиць».

Під час тестування службою кримінального аналізу технологія довела свою ефективність у розслідуванні кримінальних правопорушень та ідентифікації невстановлених трупів. Проте, існують випадки сучасні коли системи спостереження із застосуванням штучного інтелекту порушують права людини [60]. Звідси виникає питання щодо дотримання основних прав і свобод людини, а також подальшого правового врегулювання використання згаданої технології [61]. Проблема полягає в потенційних і реальних конфліктах між публічними і приватними інтересами, що є актуальним та принциповим для країн на шляху до ЄС. Наприклад, у Великій Британії поліція за допомогою

результатів вуличних камер спостереження спробувала розпізнати особу, яка намагалася вчинити самогубство, і зображення потрапили до місцевої газети, що було визнано за поширення та використання персональної інформації без згоди особи.

Сучасні технологічні можливості НПУ було отримано завдяки спільним зусиллям керівництва блоку кримінальної поліції, власників зазначених продуктів та міжнародних партнерів. Засоби розпізнавання можуть мати іноземне або українське походження та не є спеціалізованими розвідувальними або шпигунськими засобами.

Результати тестового використання цієї технології вказують на її ефективність у встановленні 2022 року ідентичності 97 трупів та більше 1800 осіб, які становили оперативний чи слідчий інтерес. УКА ГУНП в м. Києві вже розширили спектр програмного забезпечення для тестування цієї технології. ПКА ГУНП в областях також використано цю технологію. Однак варто вказати, що існують випадки, коли критичний стан трупів не дозволяв ефективно використовувати цю технологію, наприклад, у місті Буча Київської області.

Для розробки концепції використання технології розпізнавання обличчя поліцією в умовах воєнного стану необхідно вирішувати такі питання: дотримання основних конституційних прав та свобод людини, етичне ставлення до приватного життя та персональних даних, запобігання розголошенню персональних даних, розробка порядку використання технології розпізнавання обличчя, рівноправність приватного і публічного секторів, узгоджена взаємодія з приватним і публічним секторами, освіта та урахування сучасних стандартів і практик [62, с. 212].

Загалом, ці питання є орієнтовними і вимагають подальшої дискусії та вивчення в частині формування відповідних норм законодавства, які б забезпечили захист прав людини та ефективне використання технології розпізнавання обличчя в умовах воєнного стану.

Перспективним напрямом стає застосування технології аналізу емоцій та ризиків за голосом у випадках, коли дітей незаконно вивозять з України до рф, та доступні відеозаписи їхніх звернень.

Питання ідентифікації не обмежено лише категорією дітей через причетність дорослих до схем їх вивезення. Нагальними залишаються викриття особи, встановлення її особистих даних та виявлення ознак примусу до вчинення дій або бездіяльності, особливо у випадку перебування у заручниках, а також впровадження сучасних технологій та передових засобів.

До того ж, міжнародний досвід свідчить про існування успішних проектів із розпізнавання особистостей загиблих військовослужбовців [63].

Таким чином, охарактеризовані нами програмні рішення штучного інтелекту, експрес-аналізу ДНК, фенотипування, а також аналізу емоцій та ризиків за голосом виступають як допоміжні інструменти, що надають і референтну інформацію, і експрес-результати, які допомагають визначити подальший напрямок роботи.

Актуальні проблеми розвитку методів та інструментів кримінального аналізу в НПУ у якості одного із провідних предметів дискусій почали активно обговорюватись значною кількістю науковців та фахівців на конференціях та круглих столах з 2017 року, які безпосередньо стосувались кримінального аналізу. У більшості випадків такі дискусії пов'язувалися зі швидкими змінами у характері злочинності та розвитком технологій. Ось кілька таких проблем:

- *застарілість методів* - традиційні методи кримінального аналізу вже не відповідають сучасним вимогам, оскільки злочинці використовують новітні технології для скоєння кримінальних правопорушень;

- *відповідність правовим нормам* - методи кримінального аналізу мають відповідати правовим нормам, щоб результати аналізу могли використовуватися як докази в суді; це може вимагати адаптації методів до змін у законодавстві, а також врегулювання застосування методів та інструментів у класифікаторі професій;

- *складність обробки великих даних* - сучасний кримінальний аналіз часто включає роботу з великими масивами даних, що вимагає від особи, уповноваженої на проведення кримінального аналізу, навичок роботи зі складними інструментами обробки даних та їх аналізу;

- *інтеграція різноманітних даних* - потрібно інтегрувати дані з різних джерел (відеонагляд, інтернет-трафік, бази даних, соціальні мережі тощо), що може бути складним через несумісність мереж, форматів та систем;

- *безпека даних* - захист інформації, отриманої під час кримінального аналізу, від несанкціонованого доступу або втрати;

- *протидія розслідуванням* - злочинці використовують різноманітні методи для уникнення їх виявленню: шифрування, знищення доказів, використання анонімних мереж, - що ускладнює кримінальний аналіз;

- *потреба у спеціалізованих знаннях* - необхідно мати глибокі знання не тільки в оперативно-розшуковій діяльності, кримінальному праві та процесі, криміналістиці, але й у сферах, які стосуються культури, мов, інформаційних технологій, психології, соціології тощо.

- *оновлення навчальних програм* та проведення незалежного аудиту діяльності ПКА.

Вирішення цих проблем вимагає комплексного підходу, який включає законодавчі зміни, інвестиції у новітні технології, міжнародну співпрацю та професійний розвиток правоохоронців.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Про оперативно-розшукову діяльність: Закон України від 18 лют. 1992 р. № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#n89
2. Білоус Р.В. Актуальні проблеми розбудови системи кримінального аналізу в поліцейській діяльності. *Актуальні питання діяльності кримінальної поліції (з нагоди 60-річчя ДЮІ та Дня карного розшуку)*: матеріали Всеукраїнського круглого столу (м. Маріуполь, 21 квіт. 2021 р.). Маріуполь: ДонДУВС, 2021. С. 33-36.
3. Бутко Р.Ю. Імплементація моделі поліцейської діяльності, керованої аналітикою в Україні. розвиток підрозділів кримінального аналізу в умовах сьогодення. *Імплементація ILP моделі в Україні*: матеріали круглого столу (м. Одеса, 15 берез. 2023 р.). Одеса : ОДУВС, 2023. С. 8-12.
4. Благута Р.І., Мовчан А.В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 256 с.
5. Гончарук О.М., Ісмайлов К.Ю. Кримінальний аналіз у системі правоохоронних органів України: поняття, мета й *завдання. Правовий часопис Донбасу / Law journal of Donbass*. 2023. № 2(83). С. 3-9.
6. Узлов Д.Ю., Власов О.В., Онищенко Ю.М. Інтелектуальна система кримінального аналізу даних Ricas. *Актуальні питання забезпечення публічної безпеки…*: Всеукраїнської науково-практичної конференції (м. Маріуполь, 12 трав. 2018 р.). Маріуполь, 2018. С. 365-367.
7. Про надсилання методичних рекомендацій щодо організації та проведення кримінального аналізу Національної поліції України: Лист НПУ від 26 трав. 2021 р. № 6516/01/33-2021
8. Деревягін О.О. Перспективи застосування методики кримінального аналізу у протидії кіберзлочинам. *Кібербезпека в Україні: правові та організаційні питання*: матеріали ІІ Всеукраїнської науково-практичної конференції (м. Одеса, 17 лист. 2017 р.). Одеса: ОДУВС, 2017. С. 175-176.
9. Про затвердження Положення про Департамент кримінального аналізу Національної поліції України: Наказ НПУ від 29 груд. 2019 р. № 1354
10. Про пошук активів та об'єктів права власності російської федерації та її резидентів: Лист НПУ від 10 трав. 2022 р. № 3022/02/33-2022
11. Про впровадження в діяльності підрозділів кримінального аналізу методик проведення тактичного та оперативного аналізу за різними напрямками протидії злочинності: Лист ДКА НПУ від 16 груд. 2021 р. № 6925/33/01/3-2021
12. Про впровадження в тестову експлуатацію програмно-пошукового модулю «Телефон»: Лист НПУ від 14 січ. 2021 р. № 429/02/33-2022
13. Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС: Наказ МВС України від 20 жовт. 2017 р. № 870.
14. 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://d oi.org/10.32631/pb.2021.4.07
15. Узлов Д., Струков В., Гнусов Ю. Інтелектуальні системи предикативної аналітики правоохоронних органів. *European Science*. 2023. №3(sge17-03). С. 49–68. DOI: https://doi.org/10.30890/2709-2313.2023-17-03-001
16. Кисельов А.О., Копилов Е.В., Худенко Д.М. Основи кримінального аналізу: навчальний посібник. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2023. 163 с.
17. International Association of Crime Analysts. Definition and types of crime analysis [White Paper 2014-02]. Overland Park, KS: Author. Retrieved from https://iaca.net/wp-content/uploads/2017/07/2-iacawp_2014_02_definition_types_crime_analysis.pdf
18. Тактичний кримінальний аналіз: теорія та практика; навчальний посібник / О.Є. Користін, Н.П. Свиридюк, О.М. Цільмак, О.М. Заєць, К.Ю. Ісмайлов, В.А. Некрасов; МВС України, ДНДІ, ОДУВС. Одеса: РВВ ОДУВС, 2019. 216 с.
19. Congram, M., Bell, P. & Lauch, M. (2013). Policing Transnational Organized Crime and Corruption: Exploring the Role of Communication Interception Technology (Crime Prevention and Security Management). Basingstoke: Palgrave Macmillan, 141 p. Retrieved from https://link.springer.com/chapter/10.1057/9781137333797 4/
20. Користін О.Є., Пефтієв Д.О., Пеньков С.В., Некрасов В.А. Довідник керівника поліції - поліцейська діяльність, керована розвідувальною аналітикою / ILP. Київ: «Видавництво Людмила», 2019. 120 с.
21. Ковальова О.В. Теоретико-правові засади інформаційного забезпечення досудового розслідування кримінальних правопорушень: дис. … д-ра юрид. наук : 12.00.09. Київ, 2023. 474 с.

22. Користін О.Є., Денисенко Б.А. Зміст та інтерпретація терміна «intelligence» в контексті моделі intelligence-led policing (ILP). *Південноукраїнський правничий часопис.* № 1. 2023 С. 72-79.
23. Потильчак А.О. Щодо співвідношення термінів «кримінальна розвідка» та «кримінальний аналіз». *Прикарпатський юридичний вісник*. 2017. Вип. 1(16). Т. 5, ч. 1. С. 84-88.
24. Шинкаренко І.Р. Проблеми запровадження кримінального аналізу в діяльність підрозділів кримінальної поліції: теоретико-історичне підґрунтя. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2017. № 1. С. 233-242.
25. Основи кримінального аналізу: посібник з елементами тренінгу / О.Є. Користін, С.В. Албул, А.В. Холостенко та ін. Одеса : ОДУВС, 2016. 112 с.
26. Федчак І.А. Основи кримінального аналізу: навчальний посібник. Львів: Львівський державний університет внутрішніх справ, 2021. 288 с.
27. Князєв С.М. Розвідувальна аналітика в оновленій моделі організації діяльності оперативних підрозділів Національної поліції України. *Прикарпатський юридичний вісник*. Вип. 1(22). Т. 3. 2018. С. 137-143.
28. Опендатабот / Умови користування. URL: https://opendatabot.ua/open/terms
29. Школьніков В.І. Автоматизація процесів обробки й аналізу інформації з використанням програмного забезпечення. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України*: матеріали міжвідомчої науково-практичної конференції (м. Київ, 11 серп. 2022 р.). Київ: НАВС, 2022. С. 22-26.
30. Korostelova, L. & Khudenko D. (2022). Possibilities of using transcription technology in crime analysis (in National police of Ukraine as in example. Knowledge, Education, Law, Management, 6 (50), 202-205.
31. Прокоф'єва-Янчиленко Д.М. Оцінювання загроз тяжкої та/або організованої злочинності в Україні: методичні рекомендації. Київ: МНДЦ, 2022. 44 с.
32. Карчевський М. Протидія злочинності в Україні: інфорграфіка: інтерактивний довідник. Версія 3.0. 2023. URL: https://karchevskiy.com/i-dovidnyk/
33. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «SOCTA» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»: Проект наказу МВС України від 08 лист. 2023 р. № 902.
34. Григорович О.Б., Разєнков Є.В. Інформаційно-аналітичне забезпечення діяльності підрозділів кримінальної поліції під час документування та розслідування воєнних злочинів. *Імплементація ILP моделі в Україні*: матеріали круглого столу (м. Одеса, 15 берез. 2023 р.). Одеса: ОДУВС, 2023. С. 32-34.
35. Барандич В.І. Важливість використання тактичного кримінального аналізу в діяльності аналітичних підрозділів національної поліції України. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України*: матеріали міжвідомчої науково-практичної конференції (м. Київ, 11 серп. 2022 р.). Київ: НАВС, 2022. 346 с.
36. Деякі питання ведення обліку відомостей про притягнення особи до кримінальної відповідальності та наявності судимості: Наказ МВС України від 30 берез. 2022 р. № 207.
37. СТРАТЕГІЧНА МЕТА 2.8. Населення України довіряє власну безпеку Національній поліції України / Діяльність / Міжнародна інтеграція / Євроатлантична інтеграція / Пріоритетні завдання та заходи. URL: https://www.npu.gov.ua/diyalnist/mizhnarodna-integraciya/yevroatlantichna-integraciya/prioritetni-zavdannya-ta-zahodi
38. Качунь В.А. Роль інтегрованих систем відеоспостереження у створенні надійного безпекового простору «безпечне місто» (на прикладі функціонування програмно-апаратного комплексу «САМАР»). *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України*: матеріали міжвідомчої науково-практичної конференції (м. Київ, 11 серп. 2022 р.) Київ: НАВС, 2022. С. 49-52.
39. Бикова Т.О., Кисельов А.О. Застосування соціальних мереж у кримінальному аналізі. *Актуальні питання діяльності кримінальної поліції (з нагоди 60-річчя ДЮІ та Дня карного розшуку)*: Матеріали Всеукраїнського круглого столу (м. Маріуполь, 21 квіт. 2021 р.). Маріуполь: ДонДУВС, 2021.
40. Волков Р.Р. Роль програм розпізнавання облич під час ідентифікації фігурантів кримінальних проваджень й оперативно-розшукових справ, а також невпізнаних трупів, зокрема внаслідок бойових дій. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України*: матеріали міжвідомчої науково-практичної конференції (м. Київ, 11 серп. 2022 р.). Київ: НАВС, 2022. С. 49-52.
41. Дмитренко Т.Л. Протидія глобальним викликам, пов'язаним з використанням інноваційних технологій у злочинних цілях, шляхом підвищення стандартів кримінального аналізу. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України*: матеріали міжвідомчої науково-практичної конференції (м. Київ, 11 серп. 2022 р.). Київ: НАВС, 2022. С. 57-60.
42. Шишкін І.І. Ефективне поєднання тактичного й оперативного аналізу під час розслідування злочинів, пов'язаних із відмиванням (легалізацією) майна, одержаного злочинним шляхом, і фінансуванням дій збройної агресії на території України. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України*: матеріали міжвідомчої науково-практичної конференції (м. Київ, 11 серп. 2022 р.). Київ: НАВС, 2022. С.193-195.
43. Симоненко Є.В., Лисенко А.Е., Кузін О.К. Використання сучасних інформаційних технологій під час проведення кримінального аналізу. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України*: матеріали міжвідомчої науково-практичної конференції (м. Київ, 11 серп. 2022 р.). Київ: НАВС, 2022. С. 153-155.

44. Тімошин А.С. Технології обробки великих даних кримінальному аналізі. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України*: матеріали міжвідомчої науково-практичної конференції (м. Київ, 11 серп. 2022 р.). Київ: НАВС, 2022. С.163-167.
45. Про визнання таким, що втратив чинність, наказу Міністерства внутрішніх справ України від 24 верес. 2012 р. № 825: Наказ МВС України від 17 лист. 2020 р. № 812.
46. Osint4all. Retrieved from https://start.me/p/L1rEYQ/osint4all
47. Використання інструментів та методів OSINT для отримання пошукової інформації: практичний порадник / Зоренко Д.С., Лех Р.В., Кулик Д.О., Червяков О.І. Харків: ІПЮК для СБУ, 2023. 36 с.
48. Aleksandra, Bielska, Noa Rebecca, Kurz, Yves, Baumgartner & Vytenis, Benetis. Open source intelligence. Tools and resources handbook (2020). Retrieved from https://www.computer-pdf.com/pdf/1010-open-source-intelligence-tools-and-resources-handbook.pdf
49. *Global Investigative Journalism Network*. Retrieved from https://gijn.org
50. *Bellingcat*. Retrieved from https://uk.bellingcat.com
51. Мольфар. URL: https://molfar.com
52. Про Бюро економічної безпеки України: Закон України від 28 січ. 2021 р. № 1150-IX.
53. Про внесення змін до наказу Міністерства внутрішніх справ України від 20 жовтня 2017 року № 870: Наказ МВС України від 19 лип. 2022 р. № 441.
54. Про затвердження Змін до Інструкції про організацію оперативно-розшукової діяльності та негласної роботи оперативними підрозділами Національної поліції України: Наказ МВС України від 10 берез. 2023 р. № 04.
55. Про державну реєстрацію геномної інформації людини: Закон України від 9 лип. 2022 р. № 2391-IX№.
56. Бугрінова А.В. Можливості використання сучасних програмних рішень голосового аналізу під час проведення оперативного кримінального аналізу підрозділами кримінального аналізу національної поліції України. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України*: матеріали міжвідомчої науково-практичної конференції (м. Київ, 11 серп. 2022 р.). Київ: НАВС, 2022. С. 35-38.
57. Овсянюк Д.І., Худенко Д.М. Використання підрозділами кримінального аналізу технологій розпізнавання облич та фенотипування ДНК в умовах воєнного стану. *Актуальні питання та перспективи використання оперативно-розшукових засобів у розкритті злочинів в умовах воєнного стану*: матеріали міжвідомчої науково-практичної конференції (м. Київ, 30 берез. 2023 р.). Київ: НАВС, 2023. С. 231-235.
58. Intelligence-Led Policing: The New Intelligence Architecture (September 2005). Bureau of Justice Assistance. 49 p. Retrieved from https://www.ojp.gov/pdffiles1/bja/210681.pdf
59. Конституція України: Закон України від 28 черв. 1996 р. № 254к/96-ВР.
60. Войнов М. Система розпізнавання обличчя: правові аспекти використання в Україні та в ЄС. URL: https://www.helsinki.org.ua/articles/systema-rozpiznavannia-oblychchia-pravovi-aspekty-vykorystannia-v-ukraini-ta-v-yes
61. Запаранюк А.В. Актуальні питання впровадження європейських стандартів щодо розпізнавання об'єктів та облич у кримінальному розслідуванні (на прикладі наукових розробок правозахисних організацій провідних країн). *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України*: матеріали міжвідомчої науково-практичної конференції (м. Київ, 11 серп. 2022 р.). Київ: НАВС, 2022. С. 65-68.
62. Худенко Д.М. Напрями формування концепції використання технології розпізнавання обличчя в умовах воєнного стану (на прикладі служби кримінального аналізу). *Актуальні проблеми нормативно-правового визначення статусу військовополонених*: матеріали міжвідомчої науково-практичної конференції (м. Київ, 10 листоп. 2022 р.). Київ: НАВС, 2022. С. 208-213.
63. Parabon Awarded U.S. Department of Defense (DoD) Contract to Aid Identification of Unknown Remains from Past Conflicts. Snapshot Kinship Analysis to Be Enhanced for Toughest Missing Personnel Cases. Retrieved from: https://parabon-nanolabs.com/news-events/2016/01/snapshot-afdil-contractaward.html

DOI: https://doi.org/10.36486/978-966-2310-66-5-19

Думай своєю головою, користуючись об'єктивними законами логіки. Висувай гіпотези, перевіряй докази, ніколи не приймай слова на віру й ніколи не вір, що хтось за тебе відповість на поставлене тобою ж запитання

Майкл Монро Льюїс

РОЗДІЛ 19
Статистичні методи в кримінальному аналізі

Олександр Користін

Багатьох людей лякає математика і статистика. Однак роль статистики дуже важлива для розуміння звітів, публікацій, політики та загальної інформації, яку ми обробляємо щодня. Знання статистики сьогодні стає необхідним для успішної діяльності у будь-якій сфері науки й практики.

> *Фундаментальне розуміння статистики має важливе значення для кримінального аналізу (IACA) [1].*

Аналітикам підрозділів кримінального аналізу необхідно володіти основами статистичного аналізу та принципами досліджень, щоб здійснювати глибокий аналіз даних та інформації, доступних правоохоронним органам. Аналітики повинні вміти використовувати відносно не складні, на перший погляд, але потужні, саме з точки зору аналітики, методи статистичного аналізу, для опису даних і робити висновки на їх основі.

Статистичні методи допомагають описувати та інтерпретувати дані, знаходити закономірності й робити висновки на основі великих масивів даних та вивчати причинно-наслідкові зв'язки.

ОПИСОВА СТАТИСТИКА

Описова статистика узагальнює великі обсяги даних в ефективний і зрозумілий спосіб. Ці дані можуть бути або кількісними, як, наприклад, вимірювання зросту та ваги, або якісними (категоріальними), як, наприклад, стать чи тип особистості. Величезні масиви даних, як правило, повинні бути узагальненими перш ніж вони будуть інтерпретовані людиною. Тобто, описова статистика є інструментом, що описує, узагальнює або зводить до бажаного вигляду розподіл значень окремих характеристик у сукупності.

Вимірювання, його рівні (шкали) та статистика

Одне з важливих понять, яке застосовується під час вибору статистичних показників й інтерпретації отриманих результатів – це «шкали вимірювання». Дійсно, вимірювання – це приписування чисел властивостям об'єктів для кількісного представлення відповідно до певних правил. Числа присвоюються для того, щоб зробити дані придатними для статистичного аналізу. Традиційно виділяють чотири шкали вимірювання: *номінальна, порядкова, інтервальна* та *відношення*. Ці відмінності важливі, оскільки спосіб аналізу даних залежить від того, як вони були зібрані. Кожен рівень передає різну кількість інформації.

Номінальна шкала

Номінальна шкала вимірювання – це класифікація об'єктів за набором категорій. Тобто, це процес групування предметів у класи, коли об'єкти, що належать до одного класу, є ідентичними відносно певної ознаки або властивості. Для розрізнення спостережень класам присвоюють назви або ярлики, але класам для ідентифікації також можуть присвоювати і числові коди.

> ***Наприклад**, ми можемо класифікувати респондентів опитування за сімейним станом або статтю. Сімейний стан кожного респондента може бути закодований як «одружений» або «неодружений». За статтю кожен респондент кодується як «чоловік» або «жінка». Кожен респондент підпадає лише під одну класифікацію, і для кожного респондента існує відповідна категорія відповідно до його раси та статі. Хоча ми можемо присвоїти числовий код кожній категорії (наприклад, «1» для чоловіків і «2» для жінок), цей числовий код все одно сприймається як номінальні дані – не існує логічного способу впорядкувати їх або виконати з ними обчислення [1].*

Порядкова шкала

Порядкове вимірювання має місце тоді, коли числа, які позначають категорії об'єктів, можливо порівнювати, використовуючи відношення «більше», «такий самий» та «менше». Цей ступінь різниці вказує на порядок або ранжування між категоріями. Категорії певним чином впорядковані, але фактична відстань між цими порядками невідома і не має значення.

> ***Прикладами** порядкової шкали можуть бути: думка про поліцію, серйозність злочинів або рівень страху. Шкали відповідей, такі як «добре, краще, найкраще», «згоден, нейтрально, не згоден» або «дуже малоймовірно, малоймовірно, не визначився, ймовірно, дуже ймовірно», є поширеними показниками порядкової шкали [1].*

Інтервальна шкала

Інтервальне вимірювання складається з усіх характеристик номінального та порядкового вимірювання. Крім того, інтервальний рівень передбачає, що осмисленою є операція порівняння інтервалів (тобто, різниць) між парами значень на шкалі вимірювання. Для цього має існувати одиниця вимірювання тієї властивості, яка нас цікавить. На відміну від порядкових шкал, відстань між категоріями має значення.

> ***Прикладами** інтервального вимірювання є показники температури та IQ [1].*

Шкала відношень

На додаток до всіх характеристик попередніх трьох шкал вимірювання, шкала відношень має істинну нульову точку, в якій властивість зникає. Істинна нульова точка дозволяє виміряти повну відсутність поняття, що вимірюється. Завдяки цьому можливо порівнювати між собою відношення між парами значень на шкалі.

> *Дохід, вага, час і вік є прикладами вимірювань на цій шкалі [1].*

Багато властивостей можна виміряти за допомогою різних шкал вимірювання. Наприклад, **температуру** можна виміряти за допомогою відповідних наборів відповідей для кожної шкали вимірювання:

> *Номінальна шкала*: «Холодний» або «Гарячий»
>
> *Порядкова шкала*: 1 – дуже холодний, 2 – холодний, 3 – теплий, 4 – гарячий, 5 –дуже гарячий
>
> *Інтервальна шкала*: 20 градусів Цельсія, 20 градусів Фаренгейта
>
> *Шкала відношення*: 20 градусів за шкалою Кельвіна

Міри центральної тенденції

Міри центральної тенденції є найпоширенішими різновидом описових статистик. Вони використовуються для опису властивостей «типового значення» певної сукупності даних, яким можна представити всі інші. Наприклад, «типове значення» може бути описане показником «середнє арифметичне». Ці описові індекси використовуються для відповіді на запитання, як-то «Який вік типового квартирного крадія у місті за минулий рік?». Якщо уявити собі, що множина результатів розміщена на числовій прямій віку людини, то ця властивість описуваної сукупності відображається в орієнтації результатів відносно цієї прямої. Групуються вони навколо значення 28 років чи центром є 31 рік? Різні міри центральної тенденції сукупності даних спираються на різні визначення «центрального значення на шкалі». Існує порівняно невелика кількість таких мір центральної тенденції, але основними є: *мода, медіана та середнє арифметичне*.

Мода

Мода – це таке значення у множині спостережень, яке зустрічається найбільш часто. Мода визначається шляхом безпосереднього спостереження за розподілом частот. Водночас, не будь-яка сукупність має єдину моду, тому остаточне розуміння моди має особливості, зокрема:

- *у випадку, коли усі значення в групі зустрічаються з однаковою частотою, то прийнято вважати, що група оцінок не має моди, тобто в групі (0,5; 0,5; 1,6; 1,6; 3,9; 3,9) мода не можна визначити;*
- *коли два сусідніх значення мають однакову частоту і вона є більшою частоти будь-якого іншого значення, мода є середнім цих двох значень, тобто в групі (0, 1, 1, 2, 2, 2, 3, 3, 3, 4) мода 2,5;*
- *якщо два несуміжних значення у групі мають рівні частоти і вони більші від частот будь-якого значення, то існує дві моди, тобто в групі (10, 11, 11, 11, 12, 13, 14, 14, 14, 17) модами є і 11, і 14; в такому випадку кажуть, що група оцінок є бімодальною.*

Аналогічно, якщо є більше двох однакових оцінок, розподіл є мультимодальним.

Мода вказує на бал, який найбільш часто зустрічається у розподілі частот, або інтервал у згрупованому розподілі частот. Вона надає обмежену інформацію і часто є дуже нестійкою у невеликих вибірках, тому використовується рідше за інші міри центральної тенденції. Хоча мода може засто-

совуватися до всіх чотирьох шкал вимірювання, оскільки вона використовує дуже мало інформації та є найбільш придатною для даних номінальної шкали.

Медіана

Медіана (Md) – це середина або середній бал впорядкованої за величиною сукупності значень. Це значення, яке ділить упорядковану множину даних навпіл, так що одна половина значень виявляється більше медіани, а інша – меншою, тобто, точка на лінії, в якій 50% оцінок лежать вище, а 50% нижче. Однією з сильних сторін медіани є стабільність. На відміну від середнього значення, медіана не зазнає значного впливу екстремальних значень. Екстремальні значення або «викиди» можуть траплятися на обох кінцях розподілу, але вони не впливають на медіану.

Мають місце також особливості визначення медіани:

- якщо дані містять непарну кількість різних значень, наприклад 11, 13, 18, 19, 20, то медіана є серединним (центральним) значенням для випадку, коли вони упорядковані, тобто Md = 18;

- якщо дані містять парну кількість значень, наприклад 4, 9, 13, 14, то медіана є точкою, що лежить посередині між двома центральними значеннями, коли вони впорядковані, тобто Md = (9+13)/2 = 11.

Процедура знаходження медіани в таблиці частот подібна до процедури знаходження медіани в масиві. Визначається положення медіани, використовуючи кумулятивну частоту. Потім визначається значення або інтервал пов'язаного з нею класу або інтервального групування.

Середнє

Середнє значення – це середнє арифметичне. Середнє обчислюється шляхом ділення суми значень на кількість цих значень. Розподіл даних може мати лише одне середнє значення.

Середнє корисне для даних на рівні шкали інтервалів або шкали відношень. Обчислення середнього для номінальної змінної не має сенсу. Наприклад, припустимо, що набір даних містить номінальну змінну, таку як стать, і кодується «1» для чоловіків і «2» для жінок. Якщо набір даних містить десять чоловіків і три жінки, середній бал можна теоретично обчислити за наведеною вище формулою, отримавши в результаті середній бал 1,23. Однак 1,23 не має сенсу, оскільки цифри «1» і «2» використовуються як мітки, а не як арифметичні числа.

> *Кожна міра центральної тенденції наділена характеристиками, які роблять її цінною за певних умов.*

Мода найбільш просто вираховується – її можливо визначити «на око» на графіку чи в таблиці розподілу. Крім того, для надто великих груп даних це достатньо стабільна міра центру розподілу. У багатьох симетричних розподілах значної кількості вимірювань, мода є близькою і до медіани, і до середнього.

Медіана займає проміжне положення між модою та середнім з точки зору її обрахування, якщо останнє виконується вручну. У великих масивах дані спочатку групуються, а потім визначається медіана.

Середнє множини даних передбачає переважно арифметичні операції. На величину середнього впливають значення усіх результатів. Медіана й мода не потребують для визначення усіх значень.

***Наприклад**, що відбудеться з середнім, медіаною та модою, якщо подвоїться максимальне значення у наступній множині:*

Множина	Середнє	Медіана	Мода
1: 1, 3, 3, 5, 6, 7, 8	33/7	5	3
2: 1, 3, 3, 5, 6, 7, 16	41/7	5	3

На величину середнього особливо впливають результати, які називають «викидами», тобто дані, які розміщуються далеко від більшості інших значень. Перевага це чи ні – залежить від конкретних питань, що вирішуються.

Міри розсіювання

Міри центральної тенденції дають нам уявлення про концентрацію групи значень на числовій шкалі, або про «типовий» випадок у великому наборі даних. Кожна міра дає таке значення, яке «представляє», репрезентує собою усі оцінки сукупності. У цьому випадку нехтують відмінностями, що мають місце між окремими значеннями. Але варіація є основою статистики. Для вимірювання варіації оцінок всередині сукупності необхідно використовувати інші описові статистики, зокрема, окремі статистичні характеристики, які по-різному виконують роль міри розсіювання (розмах, дисперсія, стандартне відхилення).

Розмах

Розмах вимірює на числовій шкалі відстань, в межах якої змінюються оцінки. Подібно до цього, діапазон використовується для створення групувань даних за інтервалами класів, і він також є простою мірою варіації. Діапазон показує відстань (різницю) між найвищим і найнижчим значеннями в розподілі. Оскільки він використовує крайні значення, він мало що говорить про інші значення в розподілі. Ця статистика може бути нестабільною, оскільки спирається лише на два крайні значення. Між оцінками на крайніх кінцях розподілу може бути велика відстань, але невелика варіація всередині крайніх значень [1].

***Наприклад**, розглянемо два набори даних:*

Набір даних №1: 1, 7, 7, 7, 7, 8, 8, 8, 10

Набір даних №2: 1, 3, 4, 6, 9, 9, 9, 10

У наведених вище наборах даних обидва мають діапазон 9, але очевидно, що набір даних №2 має набагато більшу варіацію значень, ніж набір даних №1.

Дисперсія

Дисперсія (у популяції позначається як σ^2 – грецька літера «сигма») – це сума квадратів відхилень кожного значення сукупності від середнього, поділена на загальну кількість значень. Інакше кажучи, це середнє значення суми всіх квадратів відхилень від середнього значення будь-якого розподілу. По суті, вона підсумовує розсіювання оцінок навколо середнього значення.

Стандартне відхилення

Мірою розсіювання, тісно пов'язаною з дисперсією, є *стандартне відхилення*, яке визначається як позитивне значення квадратного кореня з дисперсії. Стандартне відхилення вимірює середню відстань, на яку кожен елемент даних віддалений від середнього значення всіх елементів даних у розподілі. Таким чином, воно вказує на середню величину варіації щодо середнього значення. Стандартне відхилення є важливим, оскільки воно дає уявлення про те, як бали в розподілі співвідносяться з типовим, центральним. Воно також дозволяє порівнювати декілька розподілів.

Через потенційний вплив викидів середнє значення може вводити в оману. Таким чином, оцінка середніх значень разом зі стандартними відхиленнями дає краще розуміння всіх оцінок разом. Іншими словами, якщо середнє значення – це типове значення сукупності всіх спостережень, то стандартне відхилення відображає середню величину відхилення кожного окремого спостереження від середнього значення. Використовуються всі бали в розподілі. Оскільки вони базуються на середньому значенні, дисперсія та стандартне відхилення потребують даних про інтервали або рівні відношення.

***Наприклад**, визначимо дисперсію та стандартне відхилення для невеликого набору даних з шести значень: 1, 6, 12, 17, 18, 24:*

Значення	Середнє	Відхилення	Відхилення в квадраті	Дисперсія	Стандартне відхилення
1	13	-12	144	71,2	8.438009
6		-7	49		
12		-1	1		
17		4	16		
18		5	25		
24		11	121		

Почнемо з обчислення середнього значення (13), потім віднімаємо кожне значення від середнього. Це дає нам відхилення кожного значення. Зводимо кожне відхилення в квадрат і підсумовуємо квадрати (356). Потім ділимо суму квадратичних відхилень на кількість значень мінус один (у нашому випадку 6 - 1 = 5) і беремо квадратний корінь з результату. Таким чином, 71,2 є дисперсією для цього набору даних, а 8.438009 – стандартним відхиленням.

Існує три міркування щодо інтерпретації стандартного відхилення:

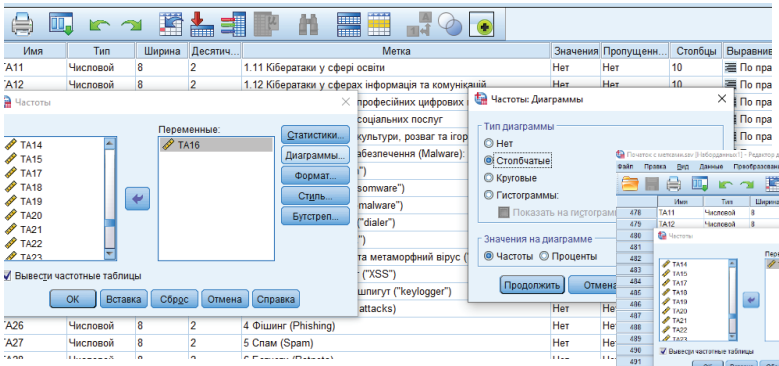
будь-яке конкретне значення стандартного відхилення не має реального інтуїтивного значення;

воно є найбільш корисним у порівняльному сенсі;

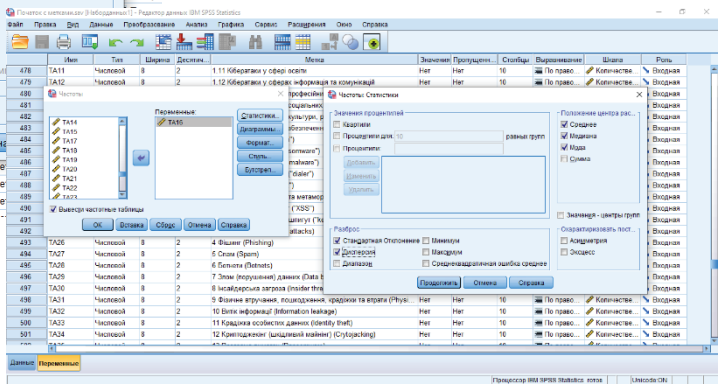
порівняння відносних значень стандартного відхилення та середнього значення показує, наскільки велика варіація в групі випадків відносно середнього значення.

> *Сучасні комп'ютерні програми, такі як Excel, SPSS, або програмне середовище R чи Python швидко обчислюють як дисперсію, так і стандартне відхилення, значною мірою усувають необхідність проходити всі ці кроки і значно спрощують процес розрахунку, залишаючи аналітику можливість та необхідність змістовної інтерпретації отриманих результатів.*

Приклад обчислення описових статистик з використанням пакету **IBM SPSS Statistics:**



1. Замовлення описових статистик: середнє, медіана, мода, дисперсія та стандартна відхилення за змінною TA16



2. Замовлення стовпчастої діаграми

```
DATASET ACTIVATE Наборданных1.
FREQUENCIES VARIABLES=TA16
  /STATISTICS=STDDEV VARIANCE MEAN MEDIAN MODE
  /BARCHART FREQ
  /ORDER=ANALYSIS.
```

3. Синтаксис за зробленим запитом

4. Отримані описові статистики з розподілом частот

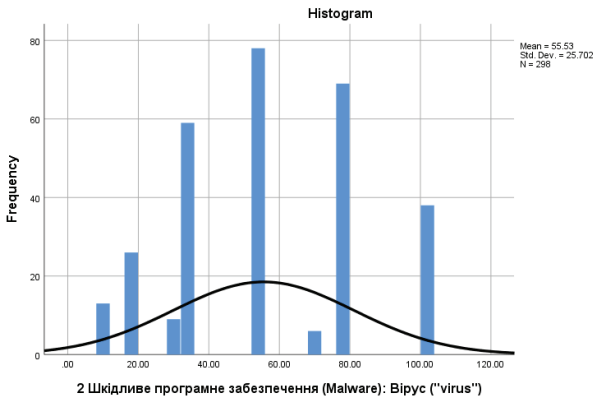
Statistics

2 Шкідливе програмне забезпечення (Malware): Вірус («virus»)

N	Valid	298
	Missing	500
Mean		55.5294
Median		52.2388
Mode		52.24
Std. Deviation		25.70201
Variance		660.594
Range		89.55

2 Шкідливе програмне забезпечення (Malware): Вірус («virus»)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	10.45	13	1.6	4.4	4.4
	19.40	26	3.3	8.7	13.1
	28.36	9	1.1	3.0	16.1
	35.82	59	7.4	19.8	35.9
	52.24	78	9.8	26.2	62.1
	68.66	6	.8	2.0	64.1
	76.12	69	8.6	23.2	87.2
	100.00	38	4.8	12.8	100.0
	Total	298	37.3	100.0	
Missing	System	500	62.7		
Total		798	100.0		



5. Гістограма з описовими статистиками та розподілом частот

СТАТИСТИЧНИЙ ВИСНОВОК

У той час як описова статистика описує характеристики конкретного набору даних, статистичний висновок використовуються для того, щоб зробити узагальнення про більшу сукупність на основі вибірки з цієї сукупності.

За допомогою описової статистики узагальнюються дані та описуються характеристики, такі як міри центральної тенденції та розсіювання. Ці методи використовуються, щоб допомогти зрозуміти конкретні характеристики певного набору даних. На відміну від них, процедури статистичного висновку використовуються для узагальнення характеристик генеральної сукупності на основі вибірки, взятої з цієї популяції (генеральної сукупності).

Щоб краще зрозуміти цю концепцію, корисно визначити деякі терміни, що за таких обставин використовуються, зокрема [1]:

> *- **Популяція (генеральна сукупність)** – це весь загальний можливий набір елементів (наприклад, випадків, людей, адрес), який цікавить дослідника. Розмір сукупності може варіюватися залежно від групи, що вивчається.*

***Прикладом** генеральної сукупності, яка часто використовується аналітиками кримінального аналізу, може бути група автомобільних крадіжок. Сукупність таких крадіжок може включати всі зареєстровані випадки у певній юрисдикції, районі чи групі, або може зосереджуватися на сукупності викликів поліції в межах однієї конкретної території у певний час.*

> *- **Вибірка** означає підмножину спостережень, взятих з генеральної сукупності.*
>
> *- **Статистичний висновок** – це перехід від результатів, отриманих на підмножині (вибірці) даних, взятих з генеральної сукупності, до оцінок характеристик цієї сукупності.*

Метою статистичного висновку є визначення характеристик генеральної сукупності, коли все, що ми маємо, – це вибірка з цієї сукупності. У наведеному вище прикладі аналітика можуть попросити визначити певну характеристику автомобільних крадіжок, яку неможливо отримати з бази даних масово (наприклад, змінну, яка не може бути надійно зафіксована під час процесу звітності).

***Наприклад**, може виникнути потреба у визначенні відсотка крадіжок, в яких не було насильницьких дій. Якщо ця змінна не фіксується в базі даних, аналітик може зробити вибірку зі спеціальних звітів, щоб визначити, як часто відбуваються крадіжки без ознак насильницьких дій. Список, з якого формується вибірка, називається основою вибірки.*

Хоча вибірка може розповісти нам щось про генеральну сукупність, не всі вибірки «створені однаковими». Найпотужніший метод формування вибірки (і метод, на якому ґрунтується більшість статистичних процедур) називається *випадковим відбором*. Як випливає з назви, вибірка є випадковою, коли кожен елемент генеральної сукупності має однакову ймовірність потрапити до вибірки. Вибірку, зібрану таким методом, часто називають простою випадковою вибіркою.

За умови достатнього розміру вибірки, випадковий відбір є достатньо потужним. Хоча аналітики кримінального аналізу часто вивчають цілі групи населення, можливість використовувати підгрупу населення для визначення характеристик всієї популяції може заощадити час і дозволити дослідити ті сфери, які інакше були б неможливими.

Випадковий відбір, однак, не гарантує, що ваша вибірка та генеральна сукупність матимуть ідентичні характеристики. Насправді, випадковість може призвести до того, що вибірка не збігатиметься з генеральною сукупністю. На ймовірність того, що статистика вашої вибірки буде схожою на параметри генеральної сукупності, впливають як розмір вибірки, так і варіативність досліджуваного об'єкта.

> ***Розмір вибірки** в цьому контексті означає кількість елементів, взятих з генеральної сукупності. Чим більшою є випадкова вибірка, тим більша ймовірність того, що за інших рівних умов вона буде схожою на генеральну сукупність.*
>
> ***Варіативність** – це кількість відмінностей між значеннями у популяції. За інших рівних умов, більша варіативність вимагає більшого розміру вибірки.*

Багато з найпоширеніших статистичних процедур розроблені для даних, які в популяції характеризуються так званим «нормальним» (гаусівським) розподілом.

> ***Нормальний розподіл** – це розподіл ймовірностей, який графічно зображується класичною симетричною дзвоновидною кривою.*

Нормальний розподіл визначається кількома характеристиками.

По-перше, нормальний розподіл є унімодальним (лише один пік), водночас середнє, медіана та мода є рівними і падають точно в центрі розподілу.

По-друге, нормальний розподіл є симетричним (тобто кожна половина, поділена центральною лінією, є дзеркальним відображенням іншої половини) і не має асиметрії.

Загальна площа нормального розподілу дорівнює одиниці або 100%. Властивістю нормального розподілу є те, що певні відсотки значень потрапляють у встановлену кількість стандартних відхилень від середнього значення сукупності. Приблизно 68% значень у розподілі знаходяться в межах одного стандартного відхилення від середнього (в позитивний і негативний бік) і приблизно 95% значень знаходяться в межах двох стандартних відхилень від середнього значення. Хоча форма нормальної кривої завжди однакова, висота й ширина кривої визначаються середнім значенням і стандартним відхиленням досліджуваних даних [1].

Нормальний розподіл часто використовується в аналізі даних, оскільки великі вибірки (зазвичай 100 або більше випадків) часто мають нормальний розподіл. Ця концепція демонструється в центральній граничній теоремі:

***центральна гранична теорема** стверджує, що розподіл середніх значень безкінечної кількості незалежних випадкових вибірок однакового обсягу буде наближатися до нормального розподілу незалежно від основного розподілу генеральної сукупності.*

Це важливо, оскільки багато статистичних тестів працюють належним чином лише тоді, коли дані мають приблизно нормальний розподіл. Одним з наслідків цієї теореми є те, що аналітик може припустити, що розподіл вибіркових середніх є нормальним, якщо вибірка є достатньо великою.

Аналітик може використовувати статистичні висновки, щоб отримати цінну інформацію про одну популяцію або декілька популяцій. Так, використовуючи приклад з автомобільними крадіжками, аналітик може розробити точкову оцінку відсотка автомобільних крадіжок зі зломом.

> ***Точкова оцінка** – це одне значення на основі вибірки, яке найкраще оцінює або наближається до істинного значення в генеральній сукупності.*

У цьому випадку ми використовуємо вибірку автомобільних крадіжок для оцінки загального відсотка автомобільних крадіжок з насильницькими діями.

Статистичний висновок реалізується шляхом побудови довірчих інтервалів та перевірки статистичних гіпотез.

> ***Перевірка гіпотез** – це покроковий процес визначення дослідницького питання, визначення статистичних методів, які можуть бути використані для відповіді на нього, проведення тестів, а потім прийняття рішення щодо даних на основі результатів, отриманих на основі вибірки.*

Вибірки та популяції

Існує низка показників, які можна використовувати для опису набору даних. Часто ми не маємо доступу до всієї сукупності даних, що ускладнює обчислення описових статистик, таких як міри центральної тенденції (наприклад, середнє, медіана і мода), міри дисперсії (наприклад, розмах, дисперсія, стандартне відхилення) та інших статистичних показників, що представляють інтерес. Під час використання для опису всієї сукупності будь-яка з цих статистик називається *параметром*. І навпаки, той самий показник, розрахований на основі вибірки, називається *статистикою*. Статистика потрібна для того, щоб оцінити значення параметру. Прикладом статистики може бути середнє значення випадково відібраної вибірки (тобто, вибіркове середнє). Параметром буде середнє значення, яке можна було б розрахувати, якби ми мали доступ до всіх спостережень у популяції.

Правильно зібрані вибірки дозволяють аналітику оцінити параметри генеральної сукупності. Однак важливо пам'ятати, що ця оцінка може бути неточною, не зважаючи на випадковий характер відбору спостережень. Основним обмеженням вибірки (і узагальнюючої статистики загалом) є те, що ми не повністю виміряли генеральну сукупність, що призводить до можливості того, що наша вибірка не буде репрезентативною для генеральної сукупності [1].

Імовірнісні та неімовірнісні вибірки

Стратегії вибірки можна умовно поділити на дві великі категорії: імовірнісні та неімовірнісні вибірки. Проста випадкова вибірка, про яку ми говорили на початку цього розділу, належить до категорії імовірнісних вибірок. Імовірнісні вибірки повинні використовувати певну форму випадкового відбору. Це означає, що всі елементи генеральної сукупності або основи вибірки повинні мати відомі шанси потрапити у вибірку.

Неімовірнісні вибірки не використовують випадковий відбір під час формування вибірки. Хоча неімовірнісні вибірки можуть бути репрезентативними для генеральної сукупності, з якої вони отримані, до них не застосовуються інструменти статистичного висновку.

Найпоширеніші методи збору імовірнісних вибірок включають [1]:

- *проста випадкова вибірка,*
- *систематична випадкова вибірка,*
- *стратифікована випадкова вибірка,*
- *кластерна вибірка.*

Проста випадкова вибірка

Проста випадкова вибірка формується шляхом надання рівних шансів бути відібраним кожному елементу генеральної сукупності або вибіркової сукупності. Елементи, відібрані за допомогою цієї процедури, становлять вибірку. Випадкова вибірка може бути із заміщенням або без заміщення. У разі вибірки із заміщенням кожен елемент повертається до основи вибірки, з якої він був відібраний, після того, як він був використаний у вибірці. Це створює ситуацію, коли один і той самий елемент може бути використаний кілька разів в одній і тій самій вибірці.

Часто вибірка відбирається без заміщення. Таким чином, кожен елемент спочатку має однакові шанси бути відібраним. Однак, по мірі того, як процес формування вибірки продовжується, шанси на те, що будь-який елемент (ще не відібраний) буде відібраний, зростають.

> ***Наприклад**, припустимо, що аналітик хоче визначити характеристики, не зафіксовані в базі даних свого відомства, у вибірці зі 100 випадків викрадення автомобілів, що сталися в певному регіоні. Замість того, щоб переглянути всі 100 випадків, аналітик вирішує випадковим чином відібрати 30 крадіжок без заміщення. Спочатку будь-який автомобіль, що потрапив до вибірки, мав би шанс 1/100 бути відібраним. Після відбору цей автомобіль буде вилучений з вибірки, що дасть наступному автомобілю шанс потрапити до вибірки з імовірністю 1/99. Цей процес продовжиться, коли третій об'єкт матиме шанс 1/98 і так далі [1].*

Чому це важливо? Основна відмінність між вибіркою із заміщенням та без заміщення полягає в тому, що елементи у вибірці із заміщенням не є незалежними. Зазвичай це не має особливого значення для великих груп населення. Однак для невеликих груп населення вибірка із заміщенням може створити проблеми, пов'язані з коваріацією. У цьому контексті коваріація просто означає ступінь, до якого дві величини змінюються разом. На практиці проблеми коваріації значно зменшуються у великих вибірках .

Систематична випадкова вибірка

Систематична випадкова вибірка – це різновид простої випадкової вибірки, яка може бути корисною в ситуаціях, коли аналітик не має основи для вибірки (тобто, списку всіх спостережень, які належать до популяції).

> ***Прикладом** цього можуть бути паперові звіти, які зберігаються в шафі й не доступні в електронному вигляді. У такому випадку аналітик може вирішити взяти перший елемент (у цьому випадку – звіт), а потім відібрати кожен n-й звіт після першого. Число n зазвичай обирається шляхом ділення загальної кількості випадків на бажану кількість для вибірки. Добуток цього рівняння називається інтервалом вибірки. Наприклад, якщо аналітик хоче відібрати 50 звітів про крадіжки автомобілів з файлів, що містять 1000 звітів, він ділить 1000 на 50. Це дасть інтервал вибірки, що дорівнює 20.*
>
> *Наступним кроком у цьому процесі буде випадковий вибір числа з інтервалу вибірки (у цьому випадку від 1 до 20) і початок вибірки з цього випадково вибраного значення. Якщо наш аналітик випадково вибере 15, то він зарахує 15 справ до файлу для першого елемента вибірки. Потім аналітик продовжить, відбираючи кожен 20-й звіт у картотеці [1].*

У деяких випадках інтервал вибірки не дорівнює цілому числу. У такому випадку аналітик буде чергувати цілі числа, відбираючи кейси. Наприклад, якщо інтервал вибірки становитиме 20,5 замість 20, аналітик буде чергувати 20-й і 21-й звіти.

Стратифікована випадкова вибірка

Стратифікована випадкова вибірка може бути використана для більш ефективного отримання ймовірнісної вибірки. Це досягається шляхом використання інформації, відомої про населення до формування вибірки, для створення страт (тобто, підгруп), з яких випадковим чином відбираються елементи вибірки. Страти створюються шляхом поділу частини населення на групи відповідно до характеристик, що становлять інтерес. Потім з кожної страти випадковим чином відбирається вибірка заздалегідь визначеного розміру.

Існує низка причин для використання цього методу. Наприклад, якщо аналітику потрібна імовірнісна вибірка частини першої злочинів і він хоче переконатися, що кожен тип злочину має

достатню кількість зразків, проста випадкова вибірка повинна бути надзвичайно великою, щоб охопити злочини, які рідко трапляються: такі як вбивства, зґвалтування і пограбування. Аналітик не може бути впевненим, що всі злочини частини 1 будуть представлені у вибірці. Більш ефективною стратегією може бути стратифікація генеральної сукупності (усіх злочинів за частиною 1) за типом злочину, а потім відбір достатньої кількості елементів з кожної страти для вивчення явищ, що цікавлять дослідника. Такий тип стратифікованої випадкової вибірки називається непропорційною стратифікованою вибіркою. Цей метод використовується для того, щоб забезпечити достатню репрезентативність випадків з менших страт, і має потенціал для підвищення точності вибірки за використання фіксованих вхідних даних.

Інша форма стратифікованої вибірки називається пропорційною стратифікованою вибіркою. У пропорційній стратифікованій вибірці обсяг вибірки кожної страти визначається її часткою в генеральній сукупності. Хоча це може виглядати складно, розрахунок є дуже простим.

Розрахунок полягає в тому, що кількість випадків у стратах (тобто кількість крадіжок) ділиться на загальну кількість випадків (тобто загальну кількість злочинів за ч. 1), помножену на загальний обсяг вибірки. Потім аналітик повинен повторити цей розрахунок для кожного типу злочинів частини 1.

Пропорційна стратифікована вибірка допомагає зменшити упередженість відбору і знизити похибку, пов'язану з рандомізацією. Однак, як пропорційна, так і непропорційна стратифікована вибірка вимагає, щоб населення було поділене на страти і щоб кожен елемент сукупності перебував в одній і тільки в одній страті (тобто, елементи є взаємовиключними). Жоден елемент сукупності не може належати до двох страт. У разі стратифікації за кількома характеристиками (наприклад, за статтю, расою та етнічною приналежністю) кількість необхідних страт може швидко стати некерованою.

Кластерна вибірка

Тоді як стратифікована вибірка вимагає більше інформації про досліджувану сукупність, кластерна вибірка може бути використана для подолання обмежень у разі спроби відібрати великі групи населення. Зокрема, вона корисна, коли відсутня основа вибірки. Це може статися під час вивчення груп населення, розміщених на великих географічних територіях або розпорошених між багатьма різними організаціями.

> ***Кластерна вибірка*** *– це стратегія вибірки, яка використовується, коли необхідно відібрати природньо існуючі групи з високим ступенем однорідності, і аналітик хоче використати ці групи для більш ефективного проведення аналізу.*

Процес починається з визначення кластерів, що підлягають вивченню, а потім випадкового відбору елементів для вибірки. Кластери визначаються як природні об'єднання елементів сукупності. Кожен елемент може з'явитися лише в одному кластері.

> ***Прикладом*** *кластера, що має відношення до аналізу злочинності, може бути вибірка поліцейських через кластери поліцейських відомств або вибірка ув'язнених у групах в'язниць. Якщо аналітик опитує всі елементи (поліцейських та ув'язнених відповідно), він проводить одноступінчасту кластерну вибірку. Як варіант, аналітик може спочатку випадковим чином відібрати управління поліції або в'язниці, а потім випадковим чином відібрати працівників поліції або ув'язнених для вибірки. Це приклад багатоступеневої кластерної вибірки. Багатоступеневі кластерні вибірки можуть включати ще більше ступенів. Наприклад, дослідник або аналітик може спочатку випадковим чином відібрати кластери регіонів, потім з цих регіонів випадковим чином відібрати кластери поліцейських управлінь, а з цих управлінь випадковим чином відібрати окремих поліцейських.*

Хоча кластерна вибірка є ефективним методом опитування великих груп, які існують і природно об'єднані в кластери, вона може збільшити похибку вибірки через складність процесу.

> ***Похибка вибірки*** *– це ймовірна розбіжність вибіркової статистики з параметрами генеральної сукупності.*

Оскільки вибірки не включають усіх членів генеральної сукупності, існує ймовірність того, що між статистикою та параметром буде існувати певна різниця. Ця різниця і є похибкою вибірки.

Перевірка гіпотез

Часто дані опитувань збираються з метою проведення цільового аналізу. Нехай завданням, яке визначило керівництво для аналітика, є з'ясування взаємозв'язку ефективності розслідування кримінальних проваджень із співвідношенням аналітиків і детективів у підрозділі чи органі.

Для відповіді на це питання аналітик має визначити: *покращує чи ні співвідношення між аналітиками та детективами якість розслідувань?*

Відповідь на це дослідницьке питання потребує перевірки відповідних гіпотез. Технічно, перевірка гіпотези – це форма статистичного висновку, коли аналітик використовує набори даних для перевірки гіпотези як твердження про значення параметру. Хороша гіпотеза є дуже конкретною щодо того, що станеться або не станеться.

Припустимо, що аналітик, який взяв початкову вибірку, вважає, що більша кількість і співвідношення аналітиків підрозділів кримінального аналізу з детективами покращує якість розслідування. Однак це дуже широка гіпотеза, і її важко перевірити. Щоб допомогти звузити питання, аналітик може розглянути, підходи вимірювання «покращення розслідувань». Відповідь на це друге питання може полягати в тому, що детективи, які отримують більше допомоги в аналізі злочинів, з більшою ймовірністю розкривають справи. Цю концепцію можна перетворити на конкретне твердження, яке можна перевірити, та сформулювати гіпотезу так:

> *Збільшення співвідношення аналітиків до детективів покращує розслідування (за рахунок покращення показників розкриття злочинів).*

У цьому випадку залежна змінна – це показники розкриття справ, а незалежна змінна – співвідношення кількості аналітиків і детективів у відомстві. А це вже можливо перевірити, оскільки маємо залежну змінну, тобто змінну, на яку впливають, і незалежну змінну, тобто змінну, яка впливає на залежну змінну.

Водночас це також спрямоване твердження, яким стверджується, що вищий відсоток аналітиків до детективів покращить результати розслідувань, на відміну від неспрямованого твердження, яке лише вказує на різницю, але не визначає напрям впливу.

> *Спрямовані твердження називають односпрямованими тестами, тоді як неспрямовані – двоспрямованими.*

Перевіряючи гіпотезу, аналітик не «доводить» її. Це неможливо. Замість цього аналітик перевіряє нульову гіпотезу, тобто твердження, яке передбачає відсутність різниці між змінними, на відміну від дослідницької гіпотези, яка стверджує, що деяка різниця існує.

> *Наразі нульова гіпотеза буде такою: співвідношення аналітиків та детективів не впливає на розслідування (через покращення показників розкриття злочинів).*

Якщо дані демонструють хибність нульової гіпотези з достатньо високим рівнем достовірності, аналітик може відкинути нульову гіпотезу і прийняти альтернативну гіпотезу як можливу.

Перевірка нульової гіпотези базується на тому, що можливим є доведення за допомогою спостереження, аналізу або логічного аргументу, що вона є некоректною (тобто неправильною або неправдивою).

> ***Правило**: ми не можемо явно довести дослідницьку гіпотезу. Все, на що ми можемо сподіватися, – це виявити інші можливі пояснення і виключити їх.*

Багато аналітиків використовують цитату сера Артура Конан Дойля (1890) як девіз:

> *«Після того, як ви відкинете неможливе, те, що залишиться, незалежно від того, наскільки воно неймовірне, має бути правдою» (IACA) [1].*

Це те, чого намагається досягти перевірка гіпотези. Перевірка гіпотези – це аргумент зведення до абсурду, який намагається продемонструвати правдивість дослідницької гіпотези шляхом спростування нульової гіпотези. Якщо нульову гіпотезу можна спростувати, це залишає дослідницьку гіпотезу як єдину можливу альтернативу. Однак часто неможливо виключити всі потенційні конкуруючі пояснення певного явища. Через це обмеження ми не можемо довести правдивість будь-якого твердження-гіпотези. Замість цього аналітик намагається збалансувати ймовірність різних видів помилок.

Часто аналітик стикається з вибором між збільшенням ймовірності помилки першого або другого типу. Перш ніж приймати рішення щодо відхилення чи не відхилення певної нульової гіпотези, доцільно зважити відносні витрати, пов'язані з помилкою першого або другого типу. Потім аналітик може врахувати ці витрати під час визначення конкретного рівня *статистичної значущості*.

P-значення та статистична значущість

Вивчення (перевірка) *p-значення* є одним із запобіжників у прагненні зменшити похибку першого типу – спростування нульової гіпотези, коли вона є фактично вірною для популяції. Розрахунок *p* враховує розмір вибірки, варіативність даних і розмір ефекту, щоб отримати число, яке вказує, наскільки спостережувані дані узгоджуються з нульовою гіпотезою.

> ***Розмір ефекту*** *– це статистика, яка оцінює величину або вплив змінної, що нас цікавить.*

Для визначення статистичної значущості використовується p-значення.

> *Результат є статистично значущим, коли p-значення є меншим за встановлений рівень значущості, який позначається символом α (грецька літера «альфа»). У соціальних науках рівень значущості часто встановлюється на рівні α = 0.05, що означає, що p-значення, менше 0.05, є статистично значущим на рівні 0.05 [1].*

Слід зазначити, що *p-значення* не вимірює розмір ефекту та не надає жодної інформації про практичну значущість результату (наприклад, чи є ефект достатньо великим, щоб бути значущим у практичному плані).

За гіпотезою, яку визначено вище, розмір ефекту – це вплив різниці у співвідношенні аналітиків і детективів на показники розкриття злочинів. Тому краще використовувати p-значення лише як один з інструментів в арсеналі аналітика.

Перевірка гіпотез є важливим статистичним інструментом, але ним можна легко зловживати. Це пов'язано з тим, що перевірка гіпотез просто оцінює два взаємовиключних твердження щодо сукупності, використовуючи вибірку, взяту з цієї сукупності. Статистично значущий результат 1) не доводить альтернативну гіпотезу і 2) стосується лише вибірки, взятої випадковим чином з генеральної сукупності. Враховуючи те, що аналітики злочинності часто мають доступ до повної генеральної сукупності (тобто до всіх зареєстрованих випадків викрадення автомобілів), корисність цих методів може бути обмеженою.

Іншою частою помилкою є припущення, що незначущий результат вказує на те, що нульова гіпотеза, є правильною або що значущий результат показує з 95% ступенем впевненості, що альтернативна гіпотеза правильна. Важливо пам'ятати, що незначущий результат просто вказує на те, що розміру вибірки недостатньо, щоб відкинути нульову гіпотезу. Пам'ятайте, що загальним консенсусом є використання $p < .05$. Такий висновок про значущість можна перекласти так, що з 95% ступенем впевненості можна стверджувати, що це не пов'язано з випадковістю, спричиненою процесом вибірки [1].

І навпаки, значущий результат підтверджує альтернативну гіпотезу лише в тій мірі, в якій існує лише одна альтернативна можливість після того, як нульова гіпотеза відкинута. Він не робить різниці між альтернативними гіпотезами, якщо існує більше однієї альтернативної гіпотези.

У правоохоронній діяльності може виявитися, що значущість не настільки важлива, як розмір ефекту. Якщо розмір ефекту є значним, може виявитися, що навіть відносно високе значення *p* (більше за 0.05, наприклад) є достатнім приводом для інформування осіб, які приймають рішення. Важливо пам'ятати про ці міркування під час перевірки гіпотез.

СТАТИСТИЧНІ МЕТОДИ ВИЯВЛЕННЯ ТА ПЕРЕВІРКИ СТАТИСТИЧНИХ ЗВ'ЯЗКІВ

Більш складні статистичні методи, такі як кореляційний або регресійний аналіз, досліджують взаємозв'язок між двома або більшою кількістю змінних, щоб краще зрозуміти, як ці змінні пов'язані одна з одною. Використовуючи такі інструменти, як дескриптивний, кореляційний і регресійний аналіз, аналітики підрозділів кримінального аналізу можуть краще зрозуміти, як взаємодіють дані про злочинність та інші дані про громадську безпеку.

Міри тісноти зв'язку – кореляція

У наборах даних, що підлягають одно- або багатовимірному аналізу, неявно передбачається, що значення, або числа, будь-якої змінної представляють послідовно визначені міри деякого поняття або об'єкта, і що вони логічно і дефінітивно пов'язані один з одним у значущий спосіб. В іншому випадку статистичні вимірювання будуть безглуздими. Хоча цей момент може здатися очевидним, варто поставити низку запитань до будь-якого набору даних, на основі якого планується проведення аналізу, щоб переконатися, що все в порядку, перш ніж продовжувати.

Перед початком аналізу необхідно розглянути певні питання, що стосуються будь-якого набору даних.

> *Перше – чи пов'язані між собою логічно значення, що представляють змінну сутність або поняття.*

> *Друге – який тип даних, маючи на увазі, що існують статистичні операції, які підходять для даних кожного типу, і що використання невідповідних процедур призводить до недостовірних результатів.*

Третє питання полягає в тому, чи можна належним чином порівнювати значення безпосередньо одне з одним, тобто чи базуються вони на одному стандарті вимірювання.

Для розуміння зазначених вимог IACA у своєму посібнику [1] наводить кілька прикладів відповідного набору даних.

Набір даних 1. *Номери телефонів місцевих мешканців, щодо яких є невиконані ордери на арешт. Почнемо з найпростішого. Незважаючи на те, що номери телефонів виглядають як числа, насправді вони є номінальними даними – кодовими назвами з використанням цифр – і тому абсолютно непридатні для будь-яких математичних обчислень або статистики. (Впорядкувати їх для полегшення пошуку може бути корисно, але це не буде статистикою).*

Набір даних 2. *Кількість років формальної шкільної освіти, яку закінчили дорослі, заарештовані за будь-які або окремі види правопорушень. Можна сказати, що такі вимірювання «операціоналізують» концепцію освітнього рівня, тобто переводять абстракцію освіти в більш відчутний і вимірюваний формат. Незважаючи на певні обмеження, такі як труднощі з обліком різних видів навчальних програм поза межами шкільних систем або коледжів, можна сказати, що таке вимірювання репрезентативно відображає рівень освіти, а дані будуть мати тип шкали відношень. Однак може виникнути проблема з третім критерієм – критерієм «рівних умов». Якщо деякі заарештовані були надто молодими, вони ще не встигли закінчити стільки років формальної освіти, скільки старші за віком заарештовані. (Саме тому перепис населення США надає ці дані лише для осіб віком 25 років і старше). З поправкою на врахування лише заарештованих мінімального віку, ця змінна виступає як належним чином визначена єдина змінна для використання в багатовимірному аналізі з різними цілями.*

Набір даних 3. *Кількість крадіжок автотранспорту протягом певного року в містах з населенням понад 100 тис. осіб. Підрахунки будь-якого повторюваного явища, такого як тип або категорія злочину, можна вважати достовірними даними типу відношення, за умови, що злочин визначається та реєструється у досить схожий спосіб у кожному місті. Однак, очевидною проблемою тут є те, що розміри міст варіюються в широкому діапазоні, так що кількість крадіжок транспортних засобів в одному місті не може бути справедливо порівняна з кількістю крадіжок в іншому місті, яке значно відрізняється за розміром. Для того, щоб поставити випадки (міста) в рівні умови, необхідно стандартизувати набір даних шляхом перетворення кількості злочинів у коефіцієнти злочинності. Зазвичай прийнято переводити кількість злочинів у показники на 100 000 осіб. Використання таких показників дає змогу порівнювати міста з різною кількістю населення (оминаючи питання відмінностей у процедурах збору та кодування даних у різних містах).*

Набір даних 4. *Кількість скарг на порушення громадського порядку (викликів поліції або інцидентів, залежно від місцевих термінів та процедур) щомісяця в юрисдикції протягом певного періоду часу. Оскільки географічна територія залишається незмінною, кількість скарг на порушення громадського порядку (шкала відношень) є відповідними значеннями єдиного визначеного поняття (якими б нечіткими не були його межі на практиці). Ця змінна містить характеристику, яка не зустрічалася в жодному з попередніх випадків. Вона складається з двох змінних: кількості порушень та інтервалів часу.*

З перерахованих прикладів, лише набір даних 4 відповідає умовам багатовимірного аналізу, оскільки визначено дві (або більше) змінних і увага приділяється спостережуваним зв'язкам між змінними.

Таким чином, отримавши 52 щотижневих підрахунки викликів про порушення громадського порядку (або будь-яке інше повторюване явище, що нас цікавить), ми можемо визначити середнє значення, дисперсію та стандартне відхилення, а також максимальну й мінімальну кількість викликів за рік. Також ми можемо повідомити або використати в подальшому аналізі, що ми «бачили» близько 25 квартирних крадіжок на тиждень, «в середньому», плюс-мінус кілька (на основі дисперсії). Такі дескриптори можуть дати нам краще уявлення про частоту виникнення проблеми або, принаймні, полегшити її пояснення іншим. Але чи буде таке середнє значення «найкращим припущенням» щодо найбільш імовірної приблизної кількості скарг на порушення громадського порядку, які можна очікувати протягом наступного, 53-го тижня?

Використання середнього значення як центральної тенденції прогнозу (а також дисперсії) на кілька тижнів вперед є, більш за все, процедурною помилкою, бо базується на припущенні про лінійність даних, тобто, що значення даних, розподілені в часі, утворюють більш-менш пряму лінію. Але це не так, і часто не так. Суспільні явища, зокрема і злочинність та порушення громадського порядку, найчастіше характеризуються різними видами нелінійних моделей зв'язку.

Кореляцію можна описати як ступінь, до якого два або більше значення (змінні) змінюються в унісон, й зв'язок описується прямою лінією. Коли дві характеристики мають позитивну кореляцію, зі збільшенням однієї збільшується і друга. Якщо кореляція негативна, то зі збільшенням значення однієї змінної значення іншої змінної буде зменшуватися. Це називається парною кореляцією.

> *Цей зв'язок не обов'язково має бути причинно-наслідковим, але за визначенням вказує на залежність.*

Сила (тісnота) цього зв'язку вимірюється коефіцієнтом кореляції Пірсона зі значеннями від +1 (значення зростають разом) до від'ємного (-1) (зі збільшенням одного значення інше зменшується).

Значення коефіцієнту кореляції, близькі до нуля, вказують на те, що лінійна залежність між досліджуваними величинами незначна або відсутня.

Таким чином, застосування кореляції до вимірювання причинновості зв'язку може вводити в оману, виходячи з того, що:

- навіть в тих випадках коли можливим є уявити наявність причиновного зв'язку між двома змінними, що корелюють, сам по собі коефіцієнт кореляції нічого не говорить про те чи впливає одна змінна на іншу, чи навпаки;

- нерідко виявлений зв'язок існує завдяки наявності та певного зв'язку з іншими змінними;

- взаємозв'язки соціального характеру, що і характеризують злочинність, завжди надзвичайно складні й ніяким чином не можуть бути пояснені виключно однією причиною.

Хоча кореляція прямо не вказує на причиновний зв'язок, вона може слугувати ключем до розгадки причини. За певних умов на її основі можливим є сформулювати гіпотези, що перевіряються експериментально, коли можливим є контроль впливу інших змінних, що виходять за наявні межі.

Існує багато різних випадків, коли аналітики підрозділів кримінального аналізу можуть бути зацікавлені у вивченні взаємозв'язку між двома або більше змінними в поліцейських даних.

***Наприклад**, кореляцію можна дослідити між змінними, як пов'язаними, так і не пов'язаними зі злочинністю, наприклад, даними перепису населення. Хоча існує буквально тисячі змінних, доступних для аналізу на основі даних перепису населення, деякі змінні, які аналітики можуть розглянути для включення в аналіз злочинності (окрім кількості населення), включають: житло (наприклад, вільне, орендоване, багатоквартирне), транспорт/власність на транспортний засіб, дохід та зайнятість.*

Залежно від рівня шкали вимірювання та характеру розподілу даних (нормального чи ненормального) можуть використовуватися різні типи коефіцієнтів кореляції. Ці обмеження називаються припущеннями щодо природи досліджуваних даних. Порушення цих припущень може поставити під сумнів результати аналізу.

Коефіцієнт кореляції Пірсона

Метод, який зазвичай використовується для вимірювання тісноти лінійного зв'язку відносних або інтервальних змінних, відомий, на честь його автора, як коефіцієнт кореляції Пірсона, і позначається літерою «*r*».

Цей коефіцієнт кореляції, який часто називають *r* Пірсона, використовується для визначення сили та напрямку лінійного зв'язку між двома змінними. Це означає, що за умови дотримання припущень цей коефіцієнт може допомогти визначити ступінь і напрямок, в якому одна змінна змінюється по відношенню до іншої змінної. Наприклад, коли *r = 1*, існує досконала і позитивна асоціація, що означає, що зі збільшенням однієї змінної, інша зростає в унісон (створюючи пряму лінію). Коефіцієнт Пірсона матиме від'ємне значення, коли одна змінна збільшується, а інша зменшується.

Нуль означає відсутність лінійного зв'язку, що дуже малоймовірно, оскільки майже кожна можлива пара змінних демонструє принаймні незначну, випадкову кореляцію.

Як зазначалося вище, кореляція не доводить причинно-наслідковий зв'язок між змінними.

Загалом, кореляція, що наближається до 1.0 (або -1.0), вказує на сильний зв'язок, але наскільки сильним є цей зв'язок? Нам потрібен спосіб пов'язати r-бали з чимось більш відчутним. Відповідь лежить у квадраті r Пірсона, показнику r-квадрат.

Відомий як коефіцієнт детермінації, r-квадрат показує частку дисперсії однієї змінної, що пояснюється іншою змінною.

Таким чином, якщо r = 0.8, r-квадрат дорівнює 0,64, що означає «64% дисперсії Y пояснюється X». Інші 36% дисперсії залишаються під впливом інших факторів.

У прикладі щодо квартирних крадіжок коефіцієнт кореляції, r Пірсона, наприклад, становив 0,775, що дає коефіцієнт детермінації (r-квадрат) 0,601, який можна інтерпретувати як «близько 60% дисперсії пояснюється незалежною змінною». Але, очевидно, не можна сказати, що плин часу (незалежна змінна) «спричинив» зміну кількості квартирних крадіжок; що б не спричиняло

збільшення або зменшення кількості квартирних крадіжок, це точно не сам час, а якісь треті змінні, з ним пов'язані.

Існує кілька важливих припущень, яких необхідно дотримуватися за використання r Пірсона:

- *змінні, що вимірюються, повинні бути неперервними (тобто, виміряні в інтервальній шкалі або шкалі відношень);*
- *обидві змінні формують двовимірний нормальний розподіл;*
- *цей коефіцієнт є чутливим до викидів, а тому їх не повинно бути;*
- *зв'язок між двома змінними є лінійним.*

Цей приклад ілюструє два важливих міркування для аналітиків кримінального аналізу, які використовують більш досконалі статистичні методи.

По-перше, важливо вивчити дані про злочинність до застосування статистичного тесту, щоб переконатися, що вони відповідають необхідним припущенням. З даними про злочинність рідко буває легко працювати, і вони часто потребують або трансформації для забезпечення відповідності припущенню про нормальність, або непараметричного тесту.

По-друге, непараметричні дані не є нормально розподіленими.

Але існують міри кореляції, які підходять для не нормально розподілених даних.

Коефіцієнт рангової кореляції Спірмена

Кореляція Спірмена використовує ранжування змінних для мінімізації впливу викидів. Цей тест можна використовувати з двома неперервними змінними, двома порядковими змінними або однією порядковою змінною та однією неперервною змінною.

На додаток до припущень щодо r Пірсона, для використання цього тесту необхідно виконати ще два припущення:

- *змінні, що аналізуються, повинні бути парними спостереженнями;*
- *між змінними має бути монотонний зв'язок (зі збільшенням однієї змінної інша змінна або збільшується, або зменшується).*

Перевагою монотонного зв'язку є те, що залежність між даними не обов'язково має бути лінійною (дані повинні послідовно зростати та/або зменшуватися по відношенню один до одного, але не обов'язково описуватися прямою лінією).

Критерій хі-квадрат на незалежність категоріальних змінних

У наведених вище прикладах ми використовували тести зв'язків, які підходять для відносних, інтервальних та порядкових даних. Тест хі-квадрат на незалежність (зазвичай називається хі-квадрат (χ^2)) має перевагу в тому, що він підходить для номінальних/дихотомічних змінних. Під час використання цього тесту метою є визначення того, чи є дві номінальні категоріальні змінні статистично незалежними. Це просто означає, що знання однієї змінної не дає жодних знань про властивості іншої змінної.

Наприклад, вираз $\chi^2 = 596{,}983$, $p > 0{,}001$ вказує на наявність зв'язку між двома змінними, що тестуються. Але для визначення сили та напряму цього зв'язку необхідно вже застосувати відповідне вимірювання цього зв'язку.

Важливо пам'ятати, що жоден з описаних вище тестів не визначає причинно-наслідковий зв'язок. Навіть якщо зв'язок (або кореляцію) виявлено, все ще існує ймовірність того, що неідентифікована третя змінна корелює з обома факторами і спричиняє цей зв'язок.

Дисперсійний аналіз (ANOVA)

Дисперсійний аналіз корисний, коли аналітик хоче порівняти середні значення з трьох або більше незалежних вибірок, які походять з однієї або більше категорійних груп. Існує кілька типів ANOVA, які використовуються в різних ситуаціях.

Однофакторний ANOVA можна використовувати для більш ніж двох груп. Важливо, що однофакторний дисперсійний аналіз – це всеохоплююча тестова статистика. Це означає, що він лише перевіряє, чи існують значущі відмінності середніх між досліджуваними групами. Він не скаже аналітику, в чому полягають ці відмінності. Враховуючи, що аналітик може досліджувати кілька груп, може виникнути необхідність у проведенні додаткових тестів.

Існує кілька припущень, яких слід дотримуватися у разі проведення однофакторного ANOVA:

- ✓ *залежна змінна повинна бути неперервною;*
- ✓ *спостереження повинні бути незалежними одне від одного;*
- ✓ *незалежна змінна є номінальною і два або більше значень.*

Оскільки це параметричний тест, розподіл залежної змінної повинен наближатися до нормального у всіх популяціях. Нарешті, в даних не повинно бути значних викидів, а дисперсії залежної змінної мають бути однорідними в досліджуваних популяціях.

В однофакторному дисперсійному аналізі аналітик прагне порівняти кілька рівнів одного фактора. Однак можуть бути випадки, коли аналітик хоче розглянути два фактори, кожен з яких має кілька рівнів.

> ***Наприклад**, аналітик хоче дослідити вплив освіти (вимірюваної категоріально як середня школа, неповний коледж або закінчений коледж) і звання (офіцер, сержант або капітан) на моральний дух.*

Двофакторний ANOVA може визначити, чи існує ефект статистичної взаємодії між двома незалежними номінальними змінними (факторами) на залежну змінну. Використовуючи наш приклад, цей тест дозволить нам побачити, чи впливає освіта на бойовий дух і чи відрізняється вплив освіти залежно від звання.

Однак такий тест зазвичай проводять лише тоді, коли аналітик вважає, що обидві незалежні змінні (освіта і звання) певним чином взаємодіють між собою. Наприклад, аналітик може припустити, що звання впливає на моральний дух, але цей вплив залежить від рівня освіти.

Це називається ефектом взаємодії. Як і у випадку з однофакторним ANOVA, цей тест визначить статистично значущі ефекти, але також потребує подальшого аналізу.

Прогноз та оцінювання – регресійний аналіз

Кореляція вимірює відносну «відповідність» або ступінь зв'язку між двома змінними. Також цей метод дає змогу оцінити надійність будь-яких прогнозів якщо у доповнення використати якісну характеристику лінії регресії.

> *Регресійний аналіз – це метод моделювання зв'язку між залежною змінною (змінною, на яку впливають) та однією, двома або більше незалежними змінними.*

Регресійний аналіз часто використовується в процесі прогнозування, що має очевидну цінність для аналітика в кримінальному аналізі, але він також може допомогти визначити конкретні незалежні змінні, пов'язані з залежною змінною.

Регресійний аналіз використовується для встановлення причинно-наслідкового зв'язку, коли кореляція вже виявлена. Однак через низьку якість поліцейських даних, мультиколінеарність та потенційну можливість упередженості щодо пропущених змінних, до спроб виявлення причинно-во-наслідкового зв'язку слід підходити з обережністю.

Під час аналізу часових рядів основне питання полягає в тому, чи існує, і якщо так, то в якій мірі, основна тенденція, що лежить в основі роботи. Тобто, чи свідчать відомі значення даних про наявність якоїсь лінії тренду, що проходить через розкид точок даних, навіть якщо вона рідко торкається або проходить безпосередньо через будь-яку з окремих точок на графіку. Якщо таку лінію тренду можна виявити й побудувати, і якщо ця лінія виявиться достатньо якісним відображенням структури точок, то можна сказати, що вона має певний прогностичний потенціал [1].

> *По суті, регресійний аналіз - це процедура розпізнавання закономірностей, що є однією з головних цілей кримінального аналізу (IACA) [1].*

Навіть якщо аналітик рідко стикається з можливістю проведення повномасштабного регресійного аналізу, елементарне розуміння його концепцій і місця у світі наукового аналізу має виявитися цінним хоча б для того, щоб допомогти відточити свої навички мислення.

Регресійний аналіз вирішує завдання пошуку загальної закономірності, що проявляється в спостереженнях за явищами, включаючи тенденції злочинності або порушень громадського порядку, взаємозв'язки між соціально-економічними явищами і поведінкою, а також інші різноманітні й складні аспекти сфери діяльності аналітика підрозділу кримінального аналізу.

Регресія передбачає розпізнавання закономірностей і чітке, хоча й не зовсім досконале, розміщення закономірності на лінії тренду, прямій чи кривій відповідно до якоїсь іншої математичної функції. Її партнер, кореляційний аналіз, показує нам, наскільки сильним є зв'язок і до якої міри ми можемо вважати його значущим, корисним і надійним.

Таким чином, *регресійний і кореляційний аналіз* – це дві сторони однієї медалі:

> ***регресія** знаходить найкращу лінію, що проходить через скупчення точок даних, і показує, як вона виглядає;*
>
> ***кореляція** показує, наскільки сильним є лінійний зв'язок і до якої міри ви можете робити з нього висновки.*

> *За наявності достатньо сильного зв'язку лінія регресії дає можливість передбачити майбутні значення залежної змінної.*

Умовно кажучи, метою регресійного аналізу є пошук найкращої прямої лінії, що проходить через хмарку точок (рис. 19.1). Такою лінією є та, яка порівняно з усіма іншими можливими розташуваннями має найменшу дисперсію, що відображає розбіжності між фактичним розміщенням точок даних на графіку та відповідними розташуваннями на найкращій прямій лінії. Точніше кажучи, розташування лінії регресії є таким, що мінімізує суму квадратів відхилень – тобто дисперсію похибок передбачення.

Алгебраїчна формула прямої має вигляд: $y = mX+b$

де:

- m – константа, відома як коефіцієнт нахилу;

- b – константа, що представляє місце на осі y, де лінія перетинається, тобто значення y при $X = 0$.

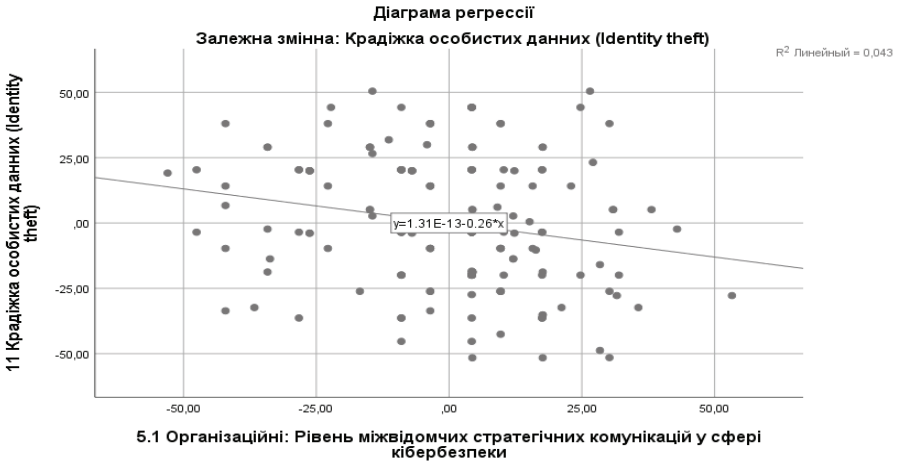


Рисунок 19.1. Діаграма регресії (*з використанням SPSS Statistics*)

> *У Microsoft Excel додавання лінії тренду до діаграми розсіювання – це просте завдання: натиснути правою кнопкою миші на одній з точок даних і вибрати «Додати лінію тренду». Програма дозволяє створювати численні типи ліній тренду (є низка варіантів нелінійної функції), в тому числі лінійну лінію тренду, яку продемонстровано (рис. 19.1). Також є можливість переглянути рівняння та його результати (а також значення R-квадрат).*

Таким чином, лінія регресії працює для знаходження набору точок (у цьому випадку лінійно вирівняних), які мінімізують квадратичні відхилення (дисперсію навколо середнього значення) фактичних значень від прогнозованих значень *Y*.

У випадку з лінією регресії дисперсія – це, по суті, те саме, за винятком того, що відхилення, які підносяться в квадрат, – це відхилення від фактичних точок до прогнозованих точок вздовж осі *y* для кожного значення *X*.

Таким чином, лінія регресії замінює середнє значення в одновимірному аналізі. Зауважимо, що стандартне відхилення було квадратним коренем з дисперсії у випадку однієї змінної, стандартна похибка, або стандартна похибка оцінки, є квадратним коренем з дисперсії у випадку регресії. Очевидно, що чим більша стандартна похибка оцінки, тим менша точність, або якість, лінії регресії, і тим менша надійність прогнозів майбутніх значень.

> *Це свідчить про здатність лінії регресії проектуватися в майбутнє і відображає той факт, що сутність математичного прогнозування полягає в регресійному аналізі (IACA) [1].*

Регресійний аналіз жодним чином не обмежується даними часових рядів. Насправді, дуже часто дві (або більше) змінні досліджуються разом, щоб визначити не тільки їхню лінію тренду (лінійну або іншу), але й ступінь зв'язку між ними, тобто їхню кореляцію. Ці процедури можна проводити з трьома або більше змінними одночасно. Коли задіяно три і більше змінних, процедури дещо ускладнюються, хоча програмне забезпечення може легко впоратися з цією проблемою.

Зазвичай, в аналізах, які використовують регресію та кореляцію, одна змінна розглядається як залежна від значень іншої, незалежної змінної, як така, що випливає з неї, з можливою, і часто оманливою, видимістю причинно-наслідкового зв'язку. Тут є певна аномалія, яку слід врахувати:

у регресійному аналізі ми будуємо дослідження таким чином, щоб припустити або шукати можливість причинново-наслідкового зв'язку – як мінімум, щоб сказати, що *«у, здається, випливає з х»* в тій чи іншій мірі. Проте неможливо визначити причинново-наслідковий зв'язок лише на основі спостережуваного патерну зв'язків [1].

Головною причиною цього є те, що можуть існувати інші фактори «під поверхнею» або поза межами безпосереднього аналізу. Ці невідомі фактори можуть впливати на значення залежної змінної, окрім тієї, що визначена як незалежна змінна. Крім того, можливо, що якась латентна змінна насправді опосередковано виявляє себе в обох досліджуваних змінних (або спричиняє їх) [1].

Звичайний хід подій у дослідницькому процесі полягає у зборі необхідних даних (достатньої кількості для обґрунтування достовірних висновків) та висуненні гіпотези, яку можна перевірити, який взаємозв'язок очікується, чому він очікується та його значущість. Таким чином встановлюється мета і сенс аналізу.

Види регресійного аналізу

Лінійна регресія

Лінійна регресія використовує існування лінійного зв'язку для прогнозування значення однієї змінної (залежної змінної) на основі значення іншої змінної (незалежної змінної). Для використання лінійної регресії необхідно, щоб обидві змінні були безперервними. Як випливає з назви, зв'язок між залежною і незалежною змінними повинен бути лінійним. Як і у випадку з кореляцією Пірсона, викиди можуть впливати на результати.

На додаток до основних критеріїв, лінійна регресія також вимагає двовимірної нормальності, гомоскедастичності та відсутності автокореляції (це кореляція змінної з самою собою в часі). Нарешті, лінійна регресія чутлива до мультиколінеарності.

> *Важливо пам'ятати, що порушення цих припущень може призвести до неточних результатів (IACA) [1].*

Існує кілька способів перевірити ці умови, але це завдання більш поглибленого додаткового вивчення, що виходить за межі цього посібника.

Лінійна регресія може бути корисною в окремих випадках, але часто наші дані не описуються лінійними закономірностями. У таких випадках використання лінійної регресії може виявитися неінформативним або навіть ввести аналітика в оману.

Логістична регресія

Логістичну регресію можна використовувати для моделювання зв'язку категоріальної залежної змінної. Це часто буває корисно, оскільки дані, які використовують аналітики, часто мають категоріальний характер (наприклад, типи арештів або демографічні змінні, такі як раса чи стать).

> ***Наприклад**, під час моделювання бінарного результату – арешт або відсутність арешту, застосування сили за поліцейським радіо-викликом або відсутність застосування сили за поліцейським радіо-викликом, аналітик може розрахувати співвідношення шансів настання події (або відсутності події), контролюючи при цьому низку незалежних змінних. Це може бути надзвичайно корисним для складання певних видів прогнозів [1].*

Пуассонівська регресія

Для моделювання даних підрахунку частоти якоїсь події можна використовувати пуасонівську регресію. З даними підрахунку може бути важко працювати через наявність нулів і відсутність від'ємних значень. Це, як правило, створює позитивно асиметричний набір даних, який часто не може бути перетворений на щось, що наближається до нормального розподілу. Пуассонівська регресія є одним з методів аналізу таких даних.

Пуассонівська регресія припускає, що наявні помилки розподілені за пуассонівським (на відміну від нормального) розподілом. За визначенням, це означає, що середнє значення й дисперсія помилок рівні. У даних про злочинність це часто не так.

> ***Наприклад**, якщо розглядати арешти за викрадення автомобілів, більшість людей не мають жодного арешту, але набагато менша група може мати десятки арештів. Це може призвести до того, що дисперсія буде більшою за середнє значення [1].*

У таких випадках доцільніше використовувати негативну біноміальну регресію.

Негативна біноміальна регресія

Негативна біноміальна регресія може бути використана, коли залежна змінна є числом (наприклад, кількість арештів за незаконне заволодіння автомобілем) і є надмірно розпорошеною.

***Прикладом** такого типу аналізу може бути ситуація, коли аналітик прогнозує кількість арештів за крадіжки з магазинів на основі характеристик підприємства (наприклад, наявність охорони під прикриттям або охорони у формі, тип магазину (біг-бокс, розмір або обсяг продажів) та певних показників соціально-економічного стану району, в якому розташоване підприємство [1].*

Аналітик може продемонструвати, що наявність охорони під прикриттям у порівнянні з охороною у формі (в такому випадку – предиктор або залежна змінна) призводить до більшої або меншої кількості арештів, незважаючи на інші фактори. За умови правильного проведення, такі аналізи можуть бути дуже корисними для запобігання злочинності або обговорення політики. Неправильно виконаний аналіз, у кращому випадку, може виставити аналітика з питань злочинності дурнем і/або некомпетентним. Використовуйте їх на свій страх і ризик [1].

Зазначене лише дуже коротко характеризує різні типи регресійного аналізу. Якщо аналітик бажає дізнатися більше про ці методи, доцільно прослухати кілька курсів зі статистики, особливо ті, що присвячені соціальним наукам.

> *Таким чином, оскільки дані стають все більш доступними, на аналітиків кримінального аналізу зростатиме тиск щодо вдосконалення способів проведення аналізу. Популярність нових «прогностичних» методів лише посилить цей тиск. Тому вивчення нових форм аналізу дає аналітикам неймовірну можливість підвищити свою цінність.*

Як зазначено у посібнику IACA «*Exploring crime analysis: Readings on essential skills*» [1], незалежно від того, чи це простий опис центральної тенденції різних факторів у ряді (наприклад, «середній час інцидентів становить 15:33; 70% злочинів сталися між 15:00 і 16:00»), чи використання регресійного аналізу для прогнозування рівня викликів на наступний рік, описова і багатовимірна статистика відіграє величезну роль в аналізі злочинності.

Кримінальні бюлетені та щорічні звіти аналітиків переповнені середніми, медіанами, модами, темпами, відсотковими змінами та кореляціями. Найчастіше ці інструменти використовуються правильно, але іноді їх застосовують некоректно, що призводить до сумнівних висновків і рекомендацій. Глибоке розуміння як описової, так і вивідної статистики має вирішальне значення для якісного аналізу та прийняття правильних рішень.

> *Важливою є потреба в осмисленні, аналізі та інтерпретації статистичних даних. Завжди пам'ятайте, що аналіз злочинності – це соціологічна сфера, а в соціології всі дані певною мірою є якісними. Статистика - це основа, а не продукт аналізу (IACA) [1].*

ПРАКТИЧНІ КЕЙСИ ВИКОРИСТАННЯ СТАТИСТИЧНИХ МЕТОДІВ В КРИМІНАЛЬНОМУ АНАЛІЗІ

Приклад 1. Аналіз інформаційних загроз в контексті гібридної війни: оцінка ризиків та прогнозування

Гібридні загрози у системі сучасної безпеки суспільства займають одне із надзвичайно важливих місць. Особливо це важливо для країн, де зовнішня агресія або інші форми збройних конфліктів знаходяться в активній фазі. Безпекова ситуація вимагає підвищення рівня обізнаності щодо інформаційних гібридних загроз та спроможності ефективної протидії їх поширенню [2]. Сучасний ризик-менеджмент передбачає аналіз та моніторинг як ключових загроз так і факторів, що формують механізми ефективної протидії таким загрозам, формування системи стійкості до загроз, прийняття управлінських рішень до підвищення спроможності протидії гібридним загрозам, уникнення вразливих компонентів у діяльності суб'єктів безпеки тощо.

***Аналітичним завданням визначено** – на основі ризик-орієнтованого підходу:*

- *оцінити інформаційні гібридні загрози у секторі цивільної безпеки,*
- *проаналізувати [3] фактори, що визначають ефективність протидії гібридним загрозам,*
- *сформувати систему індикаторів спроможності\вразливості [4], що корелюються з інформаційними гібридними загрозами та впливають на рівень зниження ризику їх поширення;*
- *на основі регресійного аналізу [5] побудувати прогнозну модель поширення інформаційних гібридних загроз за умови підвищення ключових спроможностей та зниження рівня ризику вразливості системи протидії інформаційним гібридним загрозам.*

На основі відповідної методології [2], під час оцінювання як загроз, так й індикаторів спроможності/вразливості системи протидії цим гібридним загрозам, застосовано ризик-орієнтований підхід. Крім

того, виділено узагальнюючі групи гібридних загроз у секторі цивільної безпеки, бо гібридизація може поширюватися на усі сфери суспільних відносин. Однією із ключових груп гібридних загроз у сфері цивільної безпеки є «*гібридні загрози пов'язані з інформаційним середовищем*» [6].

З усього масиву [2] ідентифікованих гібридних загроз у сфері цивільної безпеки, з інформаційним середовищем пов'язано 25 гібридних загроз, частина з яких (11) відображені в *табл. 19.2* з визначеним рівнем ризику.

Таблиця. 19.2. Оцінка ризиків поширення гібридних загроз

Гібридні загрози пов'язані з інформаційним середовищем	**№ТА**	**Risk, %**
Створення та підтримка (в т.ч. фінансова) різноманітних політичних проектів з метою розхитування соціально-політичного стану, дискредитації керівництва держави, збудження населення до громадянської непокори тощо	ТА3	**51,36**
Стимулювання та заохочення громадян України, що мешкають в прикордонних регіонах, до отримання 2-го громадянства всупереч закону	ТА4	**53,33**
Підбурювання окремих верств населення до громадянської непокори й висунення економічних та політичних вимог	ТА28	**41,10**
Контроль агресором контенту у регіонах близьких до бойових дій та прикордонних районів	ТА39	**51,04**
Провокаційна діяльність контрольованого агресором медіа ресурсу через приховування кінечного бенефіціара	ТА40	**48,14**
Просування агресивного деструктивного наративу щодо органів і працівників системи МВС через інформаційні засоби	ТА41	**41,37**
Вплив на свідомість працівників органів системи МВС, шляхом цілеспрямованої дискредитації та зниження довіри до керівництва	ТА42	**38,60**
Вплив на свідомість працівників органів системи МВС, шляхом цілеспрямованої дискредитації, спрямованої на зниження довіри до політичної еліти в державі	ТА42.4	**43,59**
Вплив на свідомість населення з метою дискредитації влади, органів і працівників системи МВС	ТА44	**49,15**
Вплив на свідомість населення з метою дискредитації влади, органів і працівників системи МВС шляхом використання цільових інформаційно-психологічних операцій	ТА44.1	**43,38**
Вплив на свідомість населення з метою дискредитації влади, органів і працівників системи МВС шляхом проведення компл інформкампаній із штучної поляризації та радикалізації суспільства, використовуючи збудженість громадян до проблеми	ТА44.4	**44,62**

Використовуючи підходи, що базуються на відображенні граничних розмірів ризиків, значні загрози, в межах 50-60%, виділено оранжевим кольором, а менш значні (40-50%) – жовтим та (менше 40%) зеленим кольорами.

Таким чином, за рівнем ризику поширення значними гібридними загрозами, пов'язаними з інформаційним середовищем, є такі:

- *стимулювання та заохочення громадян України, що мешкають в прикордонних регіонах, до отримання 2-го громадянства всупереч закону* – 53,33%;
- *створення та підтримка (в т.ч. фінансова) різноманітних політичних проєктів з метою розхитування соціально-політичного стану, дискредитації керівництва держави, збудження населення до громадянської непокори тощо* – 51,36%;
- *контроль агресором контенту в близьких до бойових дій регіонах та прикордонних районах* – 51,04%.

Незважаючи на те, що за середнім значенням, під час оцінювання ризику поширення гібридної загрози: в*плив на свідомість працівників органів системи МВС, шляхом цілеспрямованої дискредитації та зниження довіри до керівництва*, – одержано 38,6%, експертна оцінка, згідно з розподілом за усією шкалою, у 30% експертів вбачає оцінювання ризику на рівні вище 50% (*рис. 19.2*). Зазначене вказує на необхідність додаткового контролю за визначеною загрозою та певну її актуальність у сучасних умовах.

Продовжуючи аналіз, важливим є оцінювання спроможностей системи цивільної безпеки щодо зниження ризиків поширення гібридних загроз, пов'язаних з інформаційним середовищем. Для оцінювання спроможностей використано індикатори, що характеризують ефективність діяльності органів системи цивільної безпеки щодо протидії гібридним загрозам [2]. Оцінювання здійснено на основі ризик-орієнтованого підходу та враховує як ймовірність рівня ефективності, так і вплив щодо протидії гібридним загрозам.

Всього використано 152 індикатори, що характеризують ефективність (рівень можливостей, спроможностей та вразливостей) системи цивільної безпеки у протидії гібридним загрозам [2]. Гіпотетично частина з них характеризуються певним статистичним зв'язком з окремими гібридними загрозами та можуть прямо або протилежно впливати на зниження рівня ризику поширення загрози.

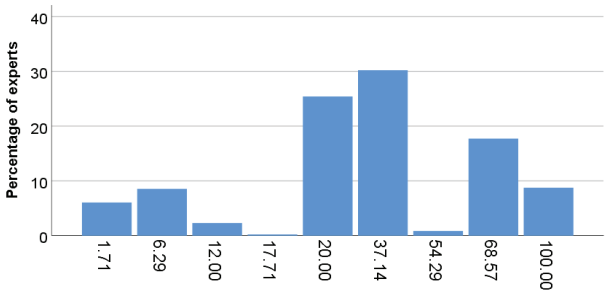


Рисунок 19.2. Вплив на свідомість працівників органів системи МВС, шляхом цілеспрямованої дискредитації та зниження довіри до керівництва

З метою підтвердження зазначеної гіпотези, на основі лінійної регресії здійснено аналіз (з *використанням SPSS Statistics*) за методом STEPWISE (відповідний синтаксис відображено на рис. 19.3), де залежною змінною використано гібридну загрозу ТА42 – в*плив на свідомість прац. органів системи МВС, шляхом цілеспрямованої дискредитації та зниження довіри до керівництва.*

```
REGRESSION
  /DESCRIPTIVES MEAN STDDEV CORR SIG N
/MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT TA42
  /METHOD=STEPWISE Rs1 Rs2 Rs3 Rs4 Rs5 Rs6 Rs7
Rs8 Rs9 Rs10 Rs11 Rs12 Rs13 Rs14 Rs15 Rs16 Rs17
Rs18 Rs19 Rs20 Rs21 Rs22 Rs23 Rs24 Rs25 Rs26 Rs27
Rs28 Rs29 Rs30 Rs31 Rs32 Rs33 Rs34 Rs35 Rs36 Rs37
Rs38 Rs39 Rs40 Rs41 Rs42 Rs43 Rs44 Rs45 Rs46 Rs47
Rs48 Rs49 Rs50 Rs51 Rs52 Rs53 Rs54 Rs55 Rs56 Rs57
Rs58 Rs59 Rs60 Rs61 Rs62 Rs63 Rs64 Rs65 Rs66 Rs67
Rs68 Rs69 Rs70 Rs71 Rw1 Rw2 Rw3 Rw4 Rw5 Rw6
Rw7 Rw8 Rw9 Rw10 Rw11 Rw12 Rw13 Rw14 Rw15
Rw16 Rw17 Rw18 Rw19 Rw20 Rw21 Rw22 Rw23 Rw24
Rw25 Ro1 Ro2 Ro3 Ro4 Ro5 Ro6 Ro7 Ro8 Ro9 Ro10
Ro11 Ro12 Ro13 Ro14 Ro15 Ro16 Ro17 Ro18 Ro19
Ro20 Ro21 Ro22 Ro23 Ro24 Ro25 Ro26 Ro27 Ro28
Ro30 Ro31 Ro32 Ro33 Ro34 Ro35 Ro36 Ro37 Ro38
Ro39 Ro40 Ro41 Ro42 Ro43 Ro44 Ro45 Ro46 Ro47
Ro48 Ro49 Ro50 Ro51 Ro53 Ro54 Ro55 Ro56 Ro57.
```

Рисунок 19.3. Синтаксис лінійної регресії із залежною змінною ТА42.

Використовуючи результати застосування лінійної регресії, була визначена статистична залежність гібридної загрози – *«вплив на свідомість працівників органів системи МВС, шляхом цілеспрямованої дискредитації та зниження довіри до керівництва»* від 5 з переліку 152 змінних, що характеризують ефективність діяльності органів системи цивільної безпеки щодо протидії гібридним загрозам (*табл. 19.3*).

Таблиця 19.3. Модель лінійної регресії із залежною змінною ТА42

Factor[a]					
Model	Unstand factors		Standard factors	т	P value
	B	Std. Err.	Beta		
(Constant)	13,886	3,333		4,188	0,000
RS44	-0,154	0,051	-0,160	-3,110	0,000
RS51	0,290	0,055	0,277	5,396	0,000
RW1	0,105	0,037	0,128	2,776	0,006
RW2	0,131	0,034	0,177	3,830	0,000
RW9	0,141	0,035	0,180	4,020	0,000

Таким чином, ключовими предикторами за результатами регресійного аналізу є:

- *RS44 - Рівень особистої стійкості співробітників органів МВС до сприйняття дезінформації;*
- *RS51 - Відповідність професійної підготовки вимогам практики на рівні початкової (базової) підготовки;*
- *RW1 - Недосконале нормативно-правове забезпечення діяльності системи МВС;*
- *RW2 - Дискредитація реформи органів МВС окремими працівниками;*
- *RW9 - Недостатній рівень професійної підготовки управлінського рівня.*

Один предиктор RS44 має негативне значення, а тому з підвищенням його рівня, ризик поширення загрози буде мати тенденцію до зниження. Інші ж предиктори з однаковим знаком у моделі лінійної регресії, а тому впливатимуть на загрозу з прямою залежністю: підвищення рівня предиктора впливатиме на підвищення означеної загрози.

Водночас надзвичайно важливим є врахування у моделі реального стану. У нашому варіанті це оцінювання вразливості або спроможності системи цивільної безпеки щодо зниження ризиків поширення інформаційних гібридних загроз. За даними дослідження

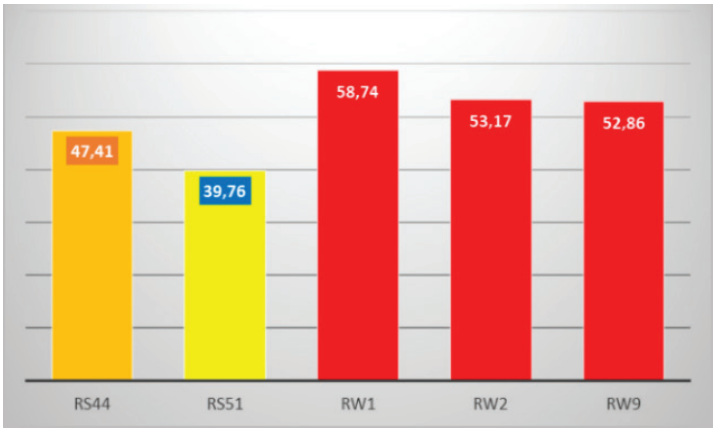


Рисунок 19.4. Оцінка ризику найзначніших предикторів.

[2] рівень ризику щодо зазначених у моделі (*табл. 19.3*) предикторів характеризується переважно вразливістю (*рис. 19.4*).

Предиктори RW1, RW2, RW9 за своїм змістом вже є вразливостями оскільки оцінюються як «слабкі сторони».

У свою чергу, предиктори RS44 та RS51, хоча за своїм змістом є явищами позитивного характеру, за оцінкою рівня ризику, яка є меншою 50%, сприймаються більше як вразливість. Така думка нами доводиться експериментально із застосуванням граничних рівнів на основі матричного аналізу [2].

Із врахуванням рівня вразливості за ключовими предикторами та використовуючи модель лінійної регресії визначено рівень ризику поширення загрози «*вплив на свідомість прац. органів системи МВС, шляхом цілеспрямованої дискредитації та зниження довіри до керівництва*» (рис. 19.5)

Model and forecast	Coeff	P value	Rating %	
(Constant)	13,886	0,000		
RS44	-0,154	0,000	47,41	-7,280920591
RS51	0,290	0,000	39,76	11,5234602
RW1	0,105	0,006	58,74	6,144196434
RW2	0,131	0,000	53,17	6,98138524
RW9	0,141	0,000	52,86	7,438466821
	TA42		**RA = 38,64 %**	

Рисунок 19.5. Оцінка ризику за залежною змінною TA42.

Coefficient	P value	Rating +/-20%	
13,886	0,000		
-0,154	0,000	67,41	-10,35239099
0,290	0,000	39,76	11,5234602
0,105	0,006	38,74	4,05219901
0,131	0,000	33,17	4,355323461
0,141	0,000	32,86	4,624063938
			RA = 28,09 %

Рисунок 19.6. Прогноз впливу на ризик поширення гібридної загрози TA42 шляхом підвищення спроможності за ключовими предикторами на 20%

Враховуючи сучасний стан вразливості системи цивільної безпеки у протидії визначеній гібридній загрозі, на основі зазначених у моделі лінійної регресії предикторів, реальний рівень ризику поширення загрози *«вплив на свідомість прац. органів системи МВС, шляхом цілеспрямованої дискредитації та зниження довіри до керівництва»* (38,69 %) є дещо вищим ніж його оцінювання на основі інтегрованого показника значень імовірності та наслідків (38,6 %). У свою чергу, розглянута модель лінійної регресії формує базові засади для прогнозу зниження рівня ризику загрози *«вплив на свідомість працівників органів системи МВС, шляхом цілеспрямованої дискредитації та зниження довіри до керівництва»* за умови підвищення спроможності системи цивільної безпеки щодо протидії інформаційним гібридним загрозам (рис. 19.6).

Таким чином, на основі оцінювання ризиків поширення *гібридних загроз, пов'язаних з інформаційним середовищем*, визначено найзначніші загрози:

- *стимулювання та заохочення громадян України, що мешкають в прикордонних регіонах, до отримання 2-го громадянства всупереч закону* – 53,33%;

- *створення та підтримка (в т.ч. фінансова) різноманітних політичних проектів з метою розхитування соціально-політичного стану, дискредитації керівництва держави, збудження населення до громадянської непокори тощо* – 51,36%;

- *контроль агресором контенту в близьких до бойових дій регіонах та прикордонних районах* – 51,04%.

Із загального переліку індикаторів (152), що характеризують ефективність правоохоронної системи у протидії гібридним загрозам, 5 з них характеризуються найбільшим впливом на загрозу «*вплив на свідомість працівників органів системи МВС, шляхом цілеспрямованої дискредитації та зниження довіри до керівництва*». Так усі предиктори за своїм рівнем оцінювання ризику характеризуються вразливістю системи, але по-різному впливають на рівень ризику визначеної загрози.

На основі моделі лінійної регресії побудовано прогноз зниження ризику поширення гібридної загрози *«вплив на свідомість прац. органів системи МВС, шляхом цілеспрямованої дискредитації та зниження довіри до керівництва»*, із врахуванням зміни рівня вразливості на 20 % (тобто підвищення спроможності) системи цивільної безпеки. За прогнозною моделлю, такі зміни ключових предикторів призводять до зменшення ризику поширення гібридної загрози *«вплив на свідомість працівників органів системи МВС, шляхом цілеспрямованої дискредитації та зниження довіри до керівництва»* з 38,64 % до 28, 09 %, більше ніж на 10 %.

Приклад 2.
Аналіз кримінального компонента гібридних загроз та прогнозування зниження ризику діяльності незаконних збройних формувань

В умовах гібридної війни у системі суспільної безпеки важливе місце займає розуміння того, що гібридизація може поширюватись на усі сфери соціальної поведінки, зокрема, не є винятком і злочинність. Враховуючи зовнішній характер загроз в умовах гібридної війни, тобто поширення зазначених загроз за безпосередньої чи опосередкованої ініціативи агресора, або третьою стороною в інтересах агресора, класичний академічний підхід до аналізу злочинності, а тим більше щодо запобігання її поширенню, є малоефективним.

За таких умов причини поширення злочинності завжди будуть мати зовнішню характеристику детермінації та найбільш імовірно, що їх провокація буде актуальною увесь період активності воєнної агресії. За таких обставин важко говорити про упереджувальний вплив на причини поширення злочинності без ліквідації факту агресії.

> *В умовах гібридної війни важливим є розуміння такого підходу, а тому можливим є виділення гіпотези щодо поширення гібридних загроз, пов'язаних з поширенням злочинності.*

Стратегії гібридної війни, крім суто збройної складової, включають принципи «рефлексивного контролю», інформаційної пропаганди, психологічного тиску, заперечення факту прямої причетності до конфлікту, заохочення дезертирства, кібератаки та різноманітні шпигунські технології [7]. На думку F. Hoffman, поширення злочинності також є елементом гібридної війни, бо криміналітет достатньо ефективно може впливати на дестабілізацію політичної ситуації та сприяти незаконним збройним формуванням [8]. А професор соціології Рущенко І.П., говорячи про гібридну війну, зазначає: соціальна дестабілізація одночасно планується й здійснюється у трьох сферах: «хаос у головах», «хаос в інституціях», «хаос на вулицях» [9].

> *Таким чином, достатньо* ***обґрунтованим є висунення і відповідної гіпотези*** *щодо необхідності врахування особливостей гібридної війни в системі кримінологічного аналізу злочинності в Україні та подальшого формування державної політики у сфері протидії злочинності із врахуванням гібридності.*

На основі факторного аналізу (*рис. 19.7*) в межах статистичної перевірки нашої гіпотези, виділено групи з найбільшою часткою поясненої відмінності окремих груп гібридних загроз.

Використовуючи додатково експертне оцінювання змісту гібридних загроз й середовища їх поширення, сформовано сутнісне сприйняття гібридних загроз з подальшим їх розподілом у 6 груп, що характеризуються так:

- *гібридні загрози, що пов'язані з інформаційним середовищем;*
- *гібридні загрози, що пов'язані з використанням кібероперацій;*
- *гібридні загрози, що пов'язані з поширенням злочинності;*
- *гібридні загрози, що пов'язані з провокуванням громадянської непокори, порушенням громадського порядку;*
- *гібридні загрози, що пов'язані з діяльністю ОКІ (об'єкти критичної інфраструктури);*
- *гібридні загрози, що пов'язані з корупцією.*



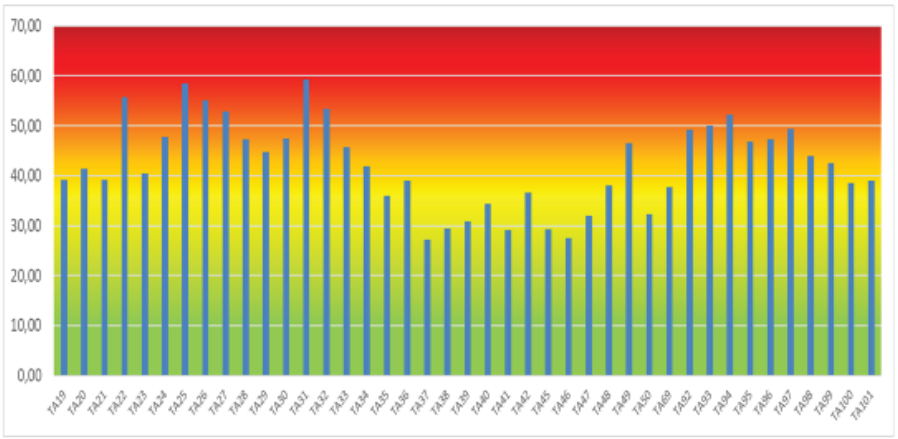
Рисунок 19.7. Результати факторного аналізу та частка поясненої відмінності окремих груп гібридних загроз

Таким чином, висунута гіпотеза щодо наявності групи гібридних загроз, пов'язаних з поширенням злочинності, має своє підтвердження і цей напрям потребує більш ґрунтовного дослідження.

Емпірична база та система індикаторів, за якою було ідентифіковано та оцінено гібридні загрози вказує на 41 вид гібридних загроз, пов'язаних з поширенням злочинності (*рис. 19.8*).

До зазначеної групи гібридних загроз увійшли: *незаконний обіг ЗБВ; діяльність незаконних збройних формувань; провокування сепаратизму; поява нових злочинних схем в економічній сфері; фінансування тероризму; терористичні акти; незаконне втручання у функціонування транспорту; діяльність ОЗУ, що спрямована на поглиблення криміногенного стану; відмивання коштів та інші.*

TA19	TA20	TA21	TA22	TA23	TA24	TA25	TA26	TA27	TA28	TA29	TA30	TA31	TA32	TA33	TA34	TA35	TA36	TA37	TA38	TA39	TA40	TA41	TA42	TA45	TA46	TA47	TA48	TA49	TA50	TA69	TA92	TA93	TA94	TA95	TA96	TA97	TA98	TA99	TA100	TA101
39,25	41,38	39,25	55,74	40,52	47,75	58,53	55,11	52,85	47,27	44,74	47,46	59,20	53,41	45,70	41,96	35,98	38,95	27,17	29,38	30,97	34,34	29,14	36,56	29,30	27,52	32,08	38,00	46,45	32,26	37,68	49,29	50,03	52,25	46,88	47,36	49,36	44,03	42,58	38,51	39,03



Найбільш значні гібридні загрози, повязані зі злочинністю	Оцінка ризику, %
TA21 Цілеспрямована діяльність організованої злочинності в інтересах агресора	39,25
TA22 Діяльність незаконних збройних формувань	55,74
TA24 Терористичні акти	47,75
TA25 Провокація сепаратизму	58,53
TA26 Незаконний обіг зброї, боєприпасів та вибухових речовин	55,11
TA28 Контрабанта озброєння	47,27
TA31 Диверсії на складах, арсеналах боєприпасів	59,20
TA35 Поширення транскордонної організованої злочинності	35,98
TA48 Ініційоване агресором поширення відмивання коштів на користь сепаратистів, інформаційних дезінформаторів тощо	38,00
TA49 Ініційоване агресором поширення фінансування тероризму	46,45

Рисунок 19.8. Гібридні загрози, повязані з поширенням злочинності

До найбільш небезпечних гібридних загроз у сфері цивільної безпеки, що пов'язані з поширенням злочинності, на основі оцінювання ризику їх поширення віднесено:

- *диверсії на складах, арсеналах боєприпасів (59,2 %),*
- *провокація сепаратизму (58,53 %),*
- *діяльність незаконних збройних формувань (55,74 %),*
- *незаконний обіг зброї, боєприпасів та вибухових речовин (55,11 %).*

> *Подальший аналіз зосереджено на одній гібридній загрозі, достатньо високого рівня ризику поширення, -* ***діяльність незаконних збройних формувань.***

Використовуючи результати оцінювання ризику щодо діяльності незаконних збройних формувань за географічною ознакою, на основі адміністративно-територіальний поділу України, побудували теплову карту, що характеризує територіальну ознаку за рівнем ризику діяльності незаконних збройних формувань в регіонах (*рис. 19.9*).

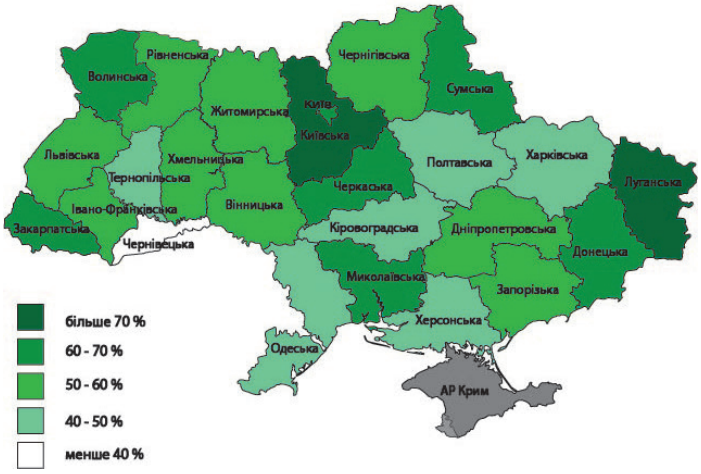


Рисунок 19.9. Теплова карта за рівнем ризику діяльності незаконних збройних формувань в регіонах України

Найбільшим рівнем ризику характеризуються Луганська та Київська області (більше 70%). Водночас також високим (в межах 60% – 70%) ризиком діяльності незаконних збройних формувань характеризуються Донецька, Миколаївська, Сумська, Черкаська, Волинська, Закарпатська області та м. Київ. За основною методикою визначення шкали оцінювання ризиків, зазначений рівень ризику в регіонах вказує на загрози надзвичайно високого рівня щодо діяльності незаконних збройних формувань саме в цих регіонах.

На основі кореляційного аналізу визначено фактори, що мають певний статистичний зв'язок із зазначеною загрозою.

Із загального переліку індикаторів (152), що характеризують ефективність правоохоронної системи у протидії гібридним загрозам, лише 53 характеризуються певним статистичним зв'язком із загрозою «діяльність незаконних збройних формувань». При чому, частина корелятів (43) має негативне значення і потенційно з підвищенням їх оціночного рівня впливатимуть на зниження означеної загрози (*табл. 19.4*). Такі фактори характеризуються позитивним змістом і, за умови рівня їх оцінювання вище 50%, визначають саме спроможності. Тобто це група факторів, що сприймаються як спроможності протидії означеній гібридній загрозі.

Таблиця 19.4. Кореляційний аналіз статистичного зв'язку діяльності незаконних збройних формувань з факторами, що характеризують спроможності

1 Оновлено та удосконалено організаційні структури органів системи МВС.	-,108*	0,017
4 Імплементовано демократичні норми та процедури провідних країн ЄС і НАТО у діяльність ПО	-,110*	0,015
5.1 Досвід МВС щодо протидії гібридним загрозам	-,122**	0,007
32 Рівень фінансового забезпечення розвитку освітньої, наукової та дослідницької діяльності у сфері НБ	-,117**	0,010
33 Рівень спроможностей навчальних та наукових установ щодо стратегічних досліджень у сфері НБ	-,101*	0,026
39 Ефективність системи моніторингу використання в Україні криміналітету в інтересах агресора	-,167**	0,000
41.3.1 Рівень використання аналіт інструментарію на оперативному рівні	-,113*	0,013
41.3.2 Рівень використання аналіт інструментарію на стратегічному рівні	-,102*	0,024

Поряд з цим, частина корелятів (10) має позитивне значення кореляції і характеризується однаковим трендом із загрозою (*табл. 19.5*). За даних умов важливою є констатація того, що фактори, поширення яких підвищують ризик діяльності незаконних збройних формувань, є негативними за своїм змістом явищами та характеризуються як вразливість системи щодо протидії гібридній загрозі «діяльність незаконних збройних формувань».

Таблиця 19.5. Кореляційний аналіз статистичного зв'язку діяльності незаконних збройних формувань з факторами, що характеризують вразливості

1 Недосконале нормативно-правове забезпечення діяльності органів системи МВС	,104*	0,022
2 Дискредитація реформи органів системи МВС окремими працівниками	,099*	0,028
3 Низькі темпи процесів реформування органів системи МВС	,130**	0,004
4 Невисока заробітна плата працівників нижчої ланки	,175**	0,000
5 Незадоволені потреби (передбачені законодавством) працівників органів системи МВС – учасників АТО	,131**	0,004
6 Окремі випадки безкарності працівників органів системи МВС	,162**	0,000
8.1 Недостатній рівень професійної підготовки управлінського (начальницького) рівня	,139**	0,002
8.2 Недостатній рівень професійної підготовки виконавського рівня (персоналу)	,103*	0,024
12 Ослаблений внутрішній контроль	,109*	0,016
23 Рівень корупційних проявів серед працівників (усіх категорій) органів системи МВС	,138**	0,002

Поряд із зазначеними результатами дослідження, важливим залишається питання визначення ключових факторів, що впливають на визначену нами гібридну загрозу та є пріоритетними щодо зменшення ризику її поширення. Зазначене аналітичне завдання базується на тому, що з переліку 152 факторів, що впливають на гібридні загрози та характеризують ефективність діяльності суб'єктів протидії гібридним загрозам, їхній вплив на конкретну загрозу щодо діяльності незаконних збройних формувань є різним. Зазначене потребує пошуку відповідного статистичного зв'язку та змістовного осмислення. З цією метою нами побудована модель лінійної регресії за методом поетапного включення, поетапного виключення та пошуку найкращих підмножин (*рис. 19.10*).

```
REGRESSION
/DESCRIPTIVES MEAN STDDEV CORR SIG N
/MISSING LISTWISE
/STATISTICS COEFF OUTS R ANOVA
/CRITERIA=PIN(.05) POUT(.10)
/NOORIGIN
/DEPENDENT TA22
/METHOD=STEPWISE Rs1 Rs2 Rs3 Rs4 Rs6 Rs7 Rs8 Rs9 Rs10 Rs11 Rs12 Rs13 Rs15 Rs16 Rs17 Rs18 Rs19 Rs20 Rs21 Rs22
Rs23 Rs24 Rs25 Rs26 Rs27 Rs28 Rs29 Rs30 Rs31 Rs32 Rs33 Rs34 Rs35 Rs36 Rs37 Rs38 Rs39 Rs40 Rs41 Rs42 Rs43 Rs44 Rs45
Rs46 Rs47 Rs48 Rs49 Rs50 Rs51 Rs52 Rs53 Rs54 Rs55 Rs56 Rs57 Rs58 Rs59 Rs60 Rs61 Rs62 Rs63 Rs64 Rs65 Rs66 Rs68 Rs69
Rs70 Rs71 Ro1 Ro2 Ro3 Ro4 Ro5 Ro6 Ro7 Ro8 Ro9 Ro10 Ro11 Ro12 Ro13 Ro14 Ro15 Ro16 Ro17 Ro18 Ro19 Ro20 Ro21 Ro22
Ro23 Ro24 Ro25 Ro26 Ro27 Ro28 Ro30 Ro31 Ro32 Ro33 Ro34 Ro35 Ro36 Ro37 Ro38 Ro39 Ro40 Ro41 Ro42 Ro43 Ro44 Ro45
Ro46 Ro47 Ro48 Ro49 Ro50 Ro51 Ro52 Ro53 Ro54 Ro55 Ro56 Ro57.
```

Рисунок 19.10. Синтаксис лінійної регресії із залежною змінною «Діяльність незаконних збройних формувань» (TA22)

Найбільш оптимальна модель лінійної регресії визначає два найбільш значущі кореляти діяльності незаконних збройних формувань (*табл. 19.6*):

- *розгорнуто на прохання Уряду України КМЄС для реформування в рамках мандату щодо розбудови спроможності органів влади,*
- *низька заробітна плата працівників нижчого рівня.*

Таблиця 19.6. Модель лінійної регресії на основі залежної змінної «Діяльність незаконних збройних формувань».

Factora					
Model	Unstand factors		Standard factors	т	P value
	B	Std. Err.	Beta		
(Constant)	51,156	2,717		18,829	0,000
розгорнуто на прохання Уряду України КМЄС для реформування в рамках мандату щодо розбудови спроможності органів влади	-0,169	0,038	-0,195	-4,435	0,000
низька заробітна плата працівників нижчого рівня	0,169	0,042	0,175	3,995	0,000

У свою чергу, спроможність за фактором «*розгорнуто на прохання Уряду України КМЄС для реформування в рамках мандату щодо розбудови спроможності органів влади*» визначена на рівні 53,57 %, а вразливість за фактором «*низька заробітна плата працівників нижчого рівня*» – 73,34 %.

Зазначене вказує на високі статистичні зв'язки залежної змінної та встановлених предикторів. Водночас змістовне осмислення такого статистичного зв'язку вказує на зниження ризику діяльності незаконних збройних формувань за умови ефективної діяльності Консультативної місії ЄС щодо розбудови спроможностей правоохоронних органів, але очікуваним є підвищення рівня досліджуваної загрози за умови зниження рівня заробітної плати працівників нижчого рівня. Зазначене має зрозумілу логіку й статистичний зв'язок закріплює змістовним зв'язком.

Враховуючи оціночні величини та застосувавши модель лінійної регресії, був визначений ризик поширення діяльності незаконних збройних формувань за умови наявного рівня спроможностей системи протидії зазначеній гібридній загрозі (*табл. 19.11*)

Таблиця 19.11. Оцінка ризику діяльності незаконних збройних формувань із врахуванням реального рівня предикторів

Модельта прогноз	**Coeff**	**P value**	**Rating %**	
(Constant)	51,156	0,000		
розгорнуто на прохання Уряду України КМЄС для реформування в рамках мандату щодо розбудови спроможності органів влади	-0,169	0,000	53,57	-9,05
низька заробітна плата працівників нижчого рівня	0,169	0,000	73,34	12,39
Поточний рівень ризику (із врахуванням спроможностей) **RA = 54,49 %**				

Потрібно зазначити, що рівень ризику діяльності незаконних збройних формувань за наявного рівня спроможностей (за встановленими предикторами) (54,49 %) є дещо нижчим ніж його оцінювання лише за інтегрованим показником двох оціночних значень – ймовірність та наслідки – (55,74 %) в статичному стані.

Поряд з цим, побудована модель лінійної регресії дає можливість розрахувати прогноз щодо зниження рівня ризику діяльності незаконних збройних формувань як гібридної загрози у секторі цивільної безпеки за умови підвищення спроможності (*розгорнуто на прохання Уряду України КМЄС для реформування в рамках мандату щодо розбудови спроможності органів влади*) – та зниження вразливості (*низька заробітна плата працівників нижчого рівня*) на 20% (*табл.* 19.12):

Coefficient	P value	Rating	
51,156	0,000		
0,169	0,000	73,57	-12,43
-0,169	0,000	53,34	9,01
RA = 47,74 %			

Таблиця 19.12. Прогноз рівня ризику діяльності незаконних збройних формувань із врахуванням підвищення спроможностей на 20%

Таким чином, на основі факторного аналізу визначено ключові групи гібридних загроз у секторі цивільної безпеки, серед яких обґрунтованою є необхідність розглядати групу гібридних загроз, пов'язаних з поширенням злочинності, з яких 41 ідентифікована, оцінений ризик їх поширення та на основі ризику встановлено найзначніші загрози.

На основі кореляційного аналізу визначено фактори, що мають певний статистичний зв'язок із зазначеною загрозою. Із загального переліку індикаторів (152), що характеризують ефективність правоохоронної системи у протидії гібридним загрозам, лише 53 характеризуються певним статистичним зв'язком із загрозою «діяльність незаконних збройних формувань».

На основі моделі лінійної регресії оцінено ризик поширення незаконних збройних формувань за умови існуючого рівня спроможності та вразливості, а також визначено пріоритетні фактори зниження цього ризику: «розгорнуто на прохання Уряду України КМЄС для реформування в рамках мандату щодо розбудови спроможності органів влади» та «низька заробітна плата працівників нижчого рівня», а також побудовано відповідну прогнозну модель.

> *За умови підвищення спроможності на 20% лише за встановленими двома індикаторами, ризик поширення діяльності незаконних збройних формувань зменшиться майже на 7%: з рівня 54,49% до 47,74%.*

ВИКОРИСТАНІ ДЖЕРЕЛА

1. 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.
2. Ковальчук Т.І., Користн О.Є., Свиридюк Н.П. Hybrid threats in the civil security sector in Ukraine. *Наука і правоохоронна*. 2019. № 3 (45). С. 69-79. DOI: doi.org/10.36486/np.2019308
3. Hua-Gang Yu, Gao-Ming Huang & Jun Gao (2010). Nonlinear Blind Source Separation Using Kernel Multi-set Canonical Correlation Analysis. *International Journal of Computer Network and Information Security*, 2 (1), 1-8. DOI: 10.5815/ijcnis.2010.01.01
4. Sonali, Sharma & Shilpa, Mahajan (2017). Design and Implementation of a Security Scheme for Detecting System Vulnerabilities. *International Journal of Computer Network and Information Security*, 9 (10), 24-32. DOI: 10.5815/ijcnis.2017.10.03
5. Mohamed Zaim, Shahrel, Sofianita, Mutalib & Shuzlina, Abdul-Rahman (2021). PriceCop–Price Monitor and Prediction Using Linear Regression and LSVM-ABC Methods for E-commerce Platform. *International Journal of Information Engineering and Electronic Business*, 13 (1), 1-14. DOI: 10.5815/ijieeb.2021.01.01
6. Oleksandr, Korystin & Nataliia, Svyrydiuk (22 March 2021). Activities of Illegal Weapons Criminal Component of Hybrid Threats. *Proceedings of the International Conference on Economics, Law and Education Research* (ELER 2021), 170, 86-91. DOI:10.2991/aebmr.k.210320.016
7. Рущенко І.П., Рущенко Ю.І. Гібридна агресія та громадянський спротив у Харкові 2014 р.: уроки першої фази російсько-української війни. *Український соціум*. 2016. № 3(58). С. 88-99.
8. Hoffman, F. (2009). Hybrid Warfare and Challenges. *JFQ*. 52, 34-39.
9. Рущенко І.П. Тактика керованого хаосу як інструмент гібридної війни. *Вісник ЛНУ імені Тараса Шевченка.* Червень 2017. № 5 (310). С. 5-29.

DOI: https://doi.org/10.36486/978-966-2310-66-5-20

Навчання ніколи не вичерпує розум.

Леонардо да Вінчі

РОЗДІЛ 20
Якісний аналіз

Олена Тихонова
Лариса Герасименко

Зміст якісного аналізу полягає в заглибленому логічному дослідженні змісту документів та інших джерел інформації. Якісний аналіз включає аналіз оперативної інформації, аналіз документів або контенту, опитувань, публікацій в соціальних мережах тощо.

> *Якісний аналіз потрібно використовувати щоб краще зрозуміти масштаб і походження закономірностей і проблем, а також здійснити поглиблену оцінку питань правоохоронної діяльності.*

Його призначення полягає у тому, щоб в масі зібраних матеріалів знайти прихований зміст, «згорнути» великий обсяг інформації [1], встановити моделі протиправної поведінки чи встановити особу, причетну до вчинення кримінального правопорушення і вирішити, у якій формі найкраще передати отриманий висновок.

Якісні методи, такі як соціологічні дослідження, фокус-групи та опитування громадян, патрульних поліцейських, інших працівників правоохоронних органів та правопорушників є придатними для збору додаткової інформації щодо кримінальної активності.

Джерелами інформації для якісного аналізу є:
- поліцейські звіти про події;
- документи про арешт або затримання особи;
- аудіо- та відеозаписи;
- фотографії;
- покази свідків і потерпілих;
- опитування офіцерів щодо їх спостережень,
- допит правопорушників, свідків, потерпілих;
- інтернет-сайти;
- засоби масової інформації;
- прямі спостереження та оперативна інформація;
- креслення, ескізи, плани будівель;
- результати прямого опитування населення окремої адміністративно-територіальної одиниці;
- випуски новин, інтерв'ю та коментарі журналістам;
- відомості з соціальних мереж, що безпосередньо або опосередковано стосується потерпілих, підозрюваних, предмету кримінального правопорушення, знаряддя вчинення кримінального правопорушення тощо.

Зазначені джерела можуть і повинні використовуватися для кращого розуміння масштабу і характеру наявних закономірностей і проблем, встановлення зв'язків між кримінальними правопорушеннями, характеристиками злочинців і конкретними способами вчинення протиправних діянь, а також для проведення поглибленої оцінки питань, пов'язаних з вчиненням кримінальних правопорушень.

> *В ході проведення якісного аналізу важливим є зосередження на факторах, що впливають на поведінку людини, а також на факторах, які опиняються під впливом такої поведінки.*

В багатьох випадках це дає можливість зрозуміти саму суть людської взаємодії, як законної, так і незаконної. Якісний аналіз також вимагає поглиблених навичок критичного мислення, щоб відмежувати важливе від неважливого та врахувати контекстну інформацію у процесі прийняття управлінських рішень.

> *Критичне мислення в кримінальному аналізі – це дисциплінованe, самостійне мислення, яке включає визнання своїх сильних і слабких сторін з метою удосконалення процесу мислення для підвищення ефективності аналітичної роботи.*

Критичне мислення це прикладна навичка, яка необхідна для того, щоб досягати кращих результатів в кримінальному аналізі. Мислення можна покращити, формулюючи якісні запитання. Питання і відповіді, є основою для критичного мислення. Навички критичного мислення також залежать від наявності відповідної бази знань.

Здатність міркувати та проводити логічне дослідження є обов'язковою умовою для критичного мислення. Поки логіка заснована на підставах, які відомі або вважаються істинними, міркування – це здатність робити висновки з високим ступенем достовірності на основі спостережень і розуміння причин і наслідків.

> *Критичне мислення передбачає використання дедуктивних, індуктивних та абдуктивних міркувань [2].*

Дедуктивне міркування – від загального до конкретного. Воно передбачає взяття загальновідомого факту і застосування його до конкретного факту або конкретного набору фактів у певній ситуації.

> *Наприклад, отримавши відомості щодо нової тенденції, зокрема, збільшення обігу певного виду наркотиків, можна зробити висновок, що збільшення випадків вуличних пограбувань у певному регіоні пов'язане з активізацією їх вживання.*

Індуктивне міркування - від конкретного до загального. Воно передбачає використання окремого факту або низки фактів щодо певного кримінального правопорушення для отримання загального пояснення.

> *Наприклад, виявлення низки окремих випадків квартирних крадіжок, що мають схожість, і класифікація їх як серії.*

Абдуктивне міркування – передбачає формулювання причин з наслідків. Воно формує пояснювальні гіпотези – це виключно логічна операція, за допомогою якої виникають нові ідеї [3, с. 124]. У випадку застосування абдукції аналітик на власний ризик обирає з низки припущень одне, на його погляд, найбільш адекватне.

> *Наприклад, спостерігається активізація незаконного збуту зброї на певній території. Аналітик формулює причини, які можуть обумовити це явище та обирає з них найбільш, на його погляд, ймовірні.*

Діалогове міркування – міркування відбувається шляхом порівняння кількох точок зору.

> *Наприклад, діалогове міркування може бути застосовано шляхом читання аналітичних звітів та висновків та вивчення різних точок зору. Використання діалогових міркувань допомагає розглянути інші точки зору та розширити усвідомлення проблем.*

Діалектичне міркування відбувається вивчення протилежних поглядів.

> *Наприклад, коли визначають що на території обслуговування діє серійний ґвалтівник розглядаються можливі аргументи проти такого висновку, щоб бути готовим відповісти на будь-які запитання щодо попереднього судження. Розгляд «аргументів проти» допомагає визначити, чи базуються висновки аналітика на відсутній або неадекватній інформації, або припущення є неправильними або нелогічними.*

Аналогічне міркування передбачає порівняння ситуації з минулою ситуацією, яка певним чином схожа на вихідну. Перегляд відповідних тематичних досліджень або пошук найкращих практик, пов'язаних із поточною проблемою, передбачає аналогію міркування, так само як і зв'язування злочинів у потенційну схему чи серію злочинів. Чим більше у аналітика досвіду у певній сфері інтересів, тим краща можливість для аналогічних міркувань завдяки постійному зростанню глибини практичних знань.

> *Спільне використання діалогового, діалектичного та аналогічного міркування в кримінальному аналізі покращує його точність і глибину.*

Ефективна діяльність аналітика можлива за умови одночасного використання навичок міркування та творчості. Таке поєднання дозволить зрозуміти яким чином кримінальні правопорушення пов'язані, розробити нову базу даних, яку можна буде використовувати в діяльності аналітика. Творча уява використовує такі методи як соціологічна уява та взаємне збагачення. Соціологічна уява передбачає розуміння події з точки зору індивіда, а індивід розуміє себе в контексті події та

суспільства. Щоб застосувати соціологічну уяву, аналітик може розглянути діяльність організованої злочинної групи в історичному або соціальному контекстах. Ця техніка може сформувати певні версії про кримінальні правопорушення, як вони вчиняються в певних місцях і періодах, і як вони стосуються конкретних осіб.

Взаємне збагачення передбачає вивчення та застосування знань і практики з інших галузей. Чим більше аналітик обізнаний в інших сферах, тим більше він може привнести в творчий процес.

> *Наприклад, методи ринкового бізнес аналізу можуть бути корисними, щоб допомогти дізнатися більше про ринки наркотиків і викрадених товарів, а знання нових технологій допомагає бути більш креативними в аналізі та відображенні інформації.*

Критичне мислення не позбавлене хибних припущень до яких призводять упередження, егоцентризм, соціоцентризм, етноцентризм.

Упередження передбачає передчасне чи несправедливе судження; його протилежністю є справедливість, яка є важливою рисою аналітика. Адже справедливість – схильність ставитися до перспектив об'єктивно, а не суб'єктивно.

Егоцентризм – схильність дивитися на все як на себе, є перешкодою розвитку критичного мислення.

Соціоцентризм, як форма упередження – віра у власне суспільство чи соціальну групу як вищу цінність. На індивідуальне мислення впливають політичні групи, релігії, соціальний статус.

Етноцентризм – схильність розглядати свою расу чи культуру як вищі упередженості.

При активному відпрацьовуванні дедуктивної та індуктивної логіки під час якісного аналізу, важливо уникати перерахованих вище пасток, оскільки вони можуть мати відчутний вплив на користувача результатів аналітичних досліджень, а згодом – на життя суспільства.

> *Якісний аналіз надає розуміння зв'язку між часом і простором – чому було вчинено кримінальне правопорушення, коли і де це відбулося, надає можливість встановити зв'язок між кримінальними правопорушеннями, конкретним способом його вчинення та характеристиками правопорушників.*

Він є ефективним інструментом для встановлення серійності кримінальних правопорушень. За результатами якісного аналізу можливо [1]:

- *ідентифікувати серію кримінальних правопорушень* – на підставі аналізу матеріалів, що утворюються під час службової діяльності працівників поліції, та порівнюючи їх з матеріалами, що утворилися раніше, а також з інформацією, отриманою з відкритих джерел;

- *розробити слідчі версії, що спрямують вектор пошуку на певних осіб, які можуть становити інтерес для досудового розслідування* – шляхом аналізу інформації, що міститься у відомчих базах даних, в матеріалах кримінальних проваджень та оперативно-розшукових справ, документах, що утворюються під час службової діяльності працівників правоохоронних органів тощо;

- *спрогнозувати ймовірний час та місце вчинення наступного кримінального правопорушення* – шляхом використання часового і просторового аналізу, у поєднанні з якісною інформацією, що використовується для прогнозування ймовірного часу і місця наступного інциденту. Оцінці підлягають особливі ознаки навколишнього середовища та дані про особу потерпілого, мету кримінального правопорушення та інші особливості вчиненого протиправного діяння;

- *посилити доказову базу проти особи підозрюваного тощо* – шляхом порівняння профілю правопорушника з інформацію, що міститься у заявах та повідомленнях про схожі кримінальні правопорушення, які мають схожі географічні, часові і поведінкові характеристики.

Додатковим способом збору якісної інформації про масштаб і характер явища є опитування громадян чи свідків. Проведення опитувань – можливість отримати корисну інформацію як усередині, так і за межами підрозділу правоохоронного органу.

> *Опитування членів громади, власників бізнесу та потерпілих від кримінальної активності дозволяє правоохоронним органам отримувати важливу інформацію, яка може запобігти злочинам і покращити громадську думку. Це якісний метод дослідження є важливим інструментом у з'ясуванні тенденцій кримінальної активності та прогнозуванні її розвитку.*

При проведенні опитувань важливо дотримуватись наступних правил:

- *питання мають бути сформульовані просто та зрозуміло;*

- уникати навідних запитань, які спрямовують респондента на найбільш бажану відповідь;
- однозначне формулювання питань закритого типу (коли обирається один із запропонованих варіантів);
- конкретне формулювання відкритих питань, щоб відповіді були зрозумілі та вимірні;
- відкриті та закриті питання завжди мають бути граматично правильними, адже помилки можуть призвести до їх хибного тлумачення;
- розміщення делікатних питань, пов'язаних з віктимізацією кримінального правопорушення, наприкінці опитування.

Групування та аналіз результатів опитування, а також формулювання відповідей має здійснюватися досвідченими аналітиками та бути досить глибоким.

Проведене опитування серед фокус-груп та здійснення на основі цього узагальнення і аналізу отриманих відповідей дає змістовне розуміння довгострокових проблем громадської безпеки. Застосовуючи якісні методи дослідження, аналітик може зібрати більше даних, ніж можна отримати лише з офіційних документів, що утворюються під час професійної діяльності працівників правоохоронних органів.

Одним із методів якісного аналізу є контент-аналіз.

Проведення контент-аналізу протягом тривалого часу дозволяє зрозуміти, що важливо для певного суспільства. При застосуванні цього методу, зміст тексту визначається як сукупність наявних у ньому відомостей, оцінок, об'єднаних у певну сукупність єдиною концепцією, задумом.

Процедура формалізованого аналізу документів починається з виділення двох одиниць аналізу: значеннєвих (якісних) і одиниць підрахунку. Мета дослідження - відшукати індикатори, що вказують на наявність у документі теми, значимої для аналізу, і такої, що розкриває зміст текстової інформації [4].

У процесі аналізу текстів плідним виявляється проблемний підхід. У цьому випадку весь текст розглядається як опис конкретної проблемної ситуації, у якій є ряд суб'єктів і відносини між ними. При формалізованому аналізі документів усебічно розглядають саму діяльність, а також виділяють її суб'єкти, цілі і мотиви вчинків, вчинених ними; обставини, причини, що породили потребу в тій або іншій діяльності; об'єкт її напрямку.

В кримінальному аналізі саме формалізований, тобто метод контент-аналізу, є найбільш доцільним для використання при опрацюванні великих масивів інформації (певні незрозумілі моменти можна з'ясувати окремо за допомогою інших якісних методів). Він є основним методом аналізу якісних показників для ідентифікації та аналізу даних з офіційних документів, а також визначення патернів та серій.

> *Контент-аналіз (англ. content analysis, нім. content-analyse, фр. analyse du contenu) - дослідницька техніка для одержання висновків шляхом аналізу змісту тексту про стани і властивості соціальної дійсності, зокрема, джерела тексту публікації.*

Він являє собою метод збору кількісних даних про досліджуване явище або процес, що містяться в документах. Під документом при цьому розуміється не тільки офіційний текст (типу інструкції або нормативно-правового акту), але все написане або вимовлене, усе, що утворилося шляхом комунікації. Контент-аналізу піддаються інтернет-джерела, газетні або журнальні статті, оголошення, телевізійні виступи, кіно- і відеозаписи, фотографії, етикетки, малюнки, інші твори мистецтва, а також офіційні документи.

Контент-аналіз не скасовує необхідності звичайного (тобто змістовного) аналізу документів. Перший доповнює другий, їхнє сполучення поглиблює розуміння змісту будь-якого тексту. Контент-аналіз дозволяє знайти в документі те, що вислизає від поверхнього погляду при його традиційному вивченні, але має важливий зміст для ефективності правоохоронної діяльності.

Контент-аналіз являє типовий приклад прикладного інформаційного аналізу тексту, що зводиться до витягу з усього розмаїття наявної в ньому інформації якихось специфічних, цікавих для аналітика компонентів і представлення їх у зручній для сприйняття і наступного аналізу формі.

Критичне мислення в кримінальному аналізі дає можливість вирішити одну з наступних задач:

- *виконати запит* на надання інформації, надавши факти без аналізу, зокрема: перелік видів кримінальних правопорушень, відповіді на питання, які включають дослідження інформації з відкритих джерел (наприклад, інтернет-джерел), пошук певних фактів тощо;

- *виконати запит* з одним або декількома питаннями, на які є обмежена кількість правильних відповідей (наприклад, який рівень насильницької злочинності у певному місті? Яка середня відстань між інцидентами? На які адреси були виклики поліції про викрадений автотранспорт? Хто конкретно вчиняє конкретне правопорушення?);

- *виконати складний запит*, для чого потрібно вибрати одну відповідь із декількох (наприклад, який район конкретного міста потребує додаткових сил та засобів для боротьби з насильством із застосуванням зброї? Які інструменти та методики слід використовувати при аналізі крадіжок з проникненням у адміністративно-територіальній одиниці? Чому ці кримінальні правопорушення відбуваються саме в цьому районі?)

Практичним кейсом аналізу якісної інформації є підготовка аналітичного дайджесту інформації, опублікованої на Internet-сторінках. За результатами якісного аналізу відкритих джерел формується *дайджест наступної структури*:

1. Новина, яка набула актуальності:
- опис проблематики;
- реакція населення;
- висновки та прогноз.

Може містити діаграму популярності за запитами у системі Google.

2. Заходи, які привернули увагу громадськості:
- інформація з мережі Інтернет (facebook-сторінки радикально налаштованих груп С14, Національний корпус, Правий сектор або інші громадські організації, які планують масові збори);
- інформація з відомчих банків даних;
- добові зведення підрозділів кримінального аналізу.

Обов'язково вказувати час, місце проведення акції, адресу місця проведення, вимоги акцій, дані організатора: анкетні дані, телефон, гіперпосилання на джерело, у т.ч. на сторінку Facebook, стислу додаткову інформацію, яка пояснює суть конфлікту.

3. Актуальні публікації в мережі Інтернет:
- події, які можуть викликати суспільний резонанс і відносяться до сфери відповідальності Національної поліції України;
- про вчинені розбої, інші резонансні злочини з використанням зброю;
- факти педофілії та інші злочини відносно дітей;
- прояви расової нетерпимості , у т. ч. відносно ромів;
- факти резонансних ДТП, де потерпілими є 2 та більше осіб;
- вбивства, напади на активістів, посадовців та громадських діячів;
- факти замінування або виявлення вибухових пристроїв;
- публікації, пов'язані з «кримінальними авторитетами».

Новини групуються за тематичними напрямами, накшталт: «Кримінальні події», «Політичні події», «Соціальні події».

4. Ситуація щодо обстрілів країни та на лінії бойового зіткнення – добові дані щодо обстрілів, постраждалих, руйнування.

Перевірити обґрунтованість результатів якісного аналізу можливо шляхом:
- *перевірки стійкості результатів*, отриманих за допомогою різних методів збору даних - порівняння даних, які зібрані певними видами якісних методів, з даними, які отримані за допомогою кількісних методів;
- *перевірки стійкості різних джерел* даних у межах одного й того ж методу – порівняння й перевірка стійкості інформації «всередині» якісних даних у різний час і різними способами (порівняння результатів спостереження і результатів інтерв'ю; порівняння того, що люди кажуть прилюдно, з тим, що вони говорять за приватних обставин; перевірка стійкості того, що говорять люди про ті самі речі у різний час; порівняння того, що говорять люди, які відіграють різні ролі у подіях, що вивчаються; перехресна перевірка інформації, отриманої під час опитування, за допомогою використання письмових джерел, які можуть підтвердити або спростувати це);
- *використання кількох аналітиків* для обробки даних - незалежне використання кількох людей, які обробляють одні й ті самі дані і потім порівнюють свої результати (наприклад, один з аналітиків може зосередитися на зборі фактів, які підтверджують гіпотезу, тоді як інший шукатиме факти, які могли б її спростувати);
- *використання кількох теорій* для інтерпретації даних дозволяє зрозуміти, як різні припущення та фундаментальні передумови впливають на результати [1].

Таким чином, якісні методи дослідження та джерела якісної інформації дозволяють аналітикам краще зрозуміти контекст, у якому відбуваються кримінальні правопорушення, і отримати більш якісну інформацію щодо розуміння історичного та географічного середовища, в якому повинні працювати працівники правоохоронних органів. Якісний аналіз слід розглядати як інструмент для кращого визначення серії злочинів, формування баз даних злочинців, збирання інформації та

оцінювання соціальних проблем, що стосуються певної адміністративно-територіальної одиниці, які впливають на тенденції злочинності, а також володіти інформацією про відносини поліції та громади, на території якої діє поліція.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Бондар В.С. Комбінація підходів щодо аналізу даних у якісному дослідженні. 2002. URL: https://core.ac.uk/download/pdf/149249641.pdf
2. Бахрушин В.Є. Методи аналізу даних: навчальний посібник для студентів. Запоріжжя: КПУ, 2011. 268 с.
3. Невельська-Гордєєва О.П., Карнаушенко С.Д. Логічна сутність абдукції як методу побудови версій. *Вісник Національного юридичного університету ім. Я. Мудрого. Серія: філософія, філософія права, політологія, соціологія*. 2022. № 2 (53). С. 120-132.
4. Бондар В.С., Допіра М.А. Розгляд методу контент-аналізу з погляду кількісно-якісних технік проведення. *Наукові записки. Соціологічні науки.* 2007. Т. 70. С. 17-26.

DOI: https://doi.org/10.36486/978-966-2310-66-5-21

Тоді лише пізнається цінність часу, коли він утрачений

Григорій Сковорода

РОЗДІЛ 21
Темпоральний аналіз

Дмитро Швець
Дмитро Афонін

ПОНЯТТЯ ТА МЕТОДИ ТЕМПОРАЛЬНОГО АНАЛІЗУ

Неможливо уявити проведення кримінального аналізу без урахування часової складової. Так, відповідно до п. 1 ч. 1 ст. 91 Кримінального процесуального кодексу України у кримінальному провадженні підлягає доказуванню *час*, як одна із складових події кримінального правопорушення [1]. Час входить до сукупності об'єктивних ознак складу злочину кримінально-правової характеристики та є елементом криміналістичної характеристики кримінального правопорушення.

Вважається що до ключових елементів криміналістичної характеристики кримінального правопорушення відносяться: особа правопорушника, особа потерпілого та місце вчинення кримінального правопорушення (злочину). Саме за наявності цих трьох ключових елементів може бути вчинене кримінальне правопорушення. У криміналістиці це зображується у вигляді «трикутнику правопорушення» або «трикутника злочину» (*рис. 21. 1*) [2]. Відсутність будь-якого з цих трьох елементів призведе до відсутності самого кримінального правопорушення. Але в цій традиційній моделі, яка враховує ключові умови вчинення злочину не передбачений саме час, який в свою чергу є четвертим ключовим елементом. Час пов'язує всі три елементи. Так, для того, щоб злочин відбувся, правопорушник, потерпілий та місце вчинення правопорушення повинні бути одночасно.



Рисунок 21.1. «Трикутник злочину», модель за якої вчиняється кримінальне правопорушення.

> ***Наприклад**, М. перебуває на щойно відкритому залізничному вокзалі, і кишеньковий злодій на ім'я С. викрадає його гаманець. Але кримінальне правопорушення (злочин) може відбутися лише при умові того, що М. та С. знаходилися на вокзалі одночасно. Так, якщо два роки тому вокзалу ще не існувало, то цей злочин не міг бути вчинений у той час. Якщо С. переховувався на вокзалі вже після 23:00, то ймовірність того, що М. або інші потенційні потерпілі також були там, є низькою, оскільки останній потяг відходить об 23:00. О 06:00 М. знаходиться на вокзалі, але в цей час там не має С., у зв'язку з тим, що він не «працює» вранці. Проте о 18:00 М. вже на вокзалі та чекає на потяг, разом з багатьма іншими потенційними потерпілими. С. також на вокзалі, отже, всі три елементи трикутника кримінального правопорушення (злочину) наявні, і ймовірність того, що воно відбудеться, висока.*

Зробивши аналіз часових періодів, пов'язаних з правопорушником, потерпілим та місцем вчинення кримінального правопорушення, можливо застосувати превентивні заходи, щодо попередження даного злочину.

Таким чином, аналіз часу та часових періодів має дуже велике значення як, зокрема, у кримінальному аналізі, так і в цілому, у протидії кримінальним правопорушенням. Даний аналіз називається темпоральним (від лат. *temporalis* – «часовий»).

> ***Темпоральний аналіз*** *– це один із напрямів кримінального аналізу, направлений на детальне дослідження різних часових періодів, конкретного часу в якому перебуває об'єкт дослідження або відбувається подія, явище, встановлення взаємозв'язків між ними та іншими елементами злочинної діяльності (особа правопорушника, особа потерпілого, місце вчинення правопорушення, спосіб вчинення правопорушення тощо), з метою ідентифікації та діагностики цих взаємозв'язків та подальшого їх використання у розслідуванні кримінальних правопорушень у якості доказів або оперативно-розшукової інформації.*

Одними із основних властивостей часу є те, що, по-перше, він постійно рухається, а по-друге, рух його відбувається тільки в одному напрямку. Ці властивості роблять час унікальним елементом кримінального аналізу, враховуючи який, можливо вирішити багато завдань щодо ідентифікації взаємозв'язків злочинної діяльності [3].

Одиниці вимірювання часу.

Перш ніж проводити темпоральний аналіз, необхідно з'ясувати, а яким чином відбувається вимірювання часу та які одиниці вимірювання існують на теперішній час. Так, сучасні одиниці вимірювання часу засновані на періодах обертання Землі навколо своєї осі і обертання навколо Сонця, а також обертання Місяця навколо Землі. Такий вибір одиниць зумовлено як історичними, так і практичними міркуваннями: необхідністю узгоджувати діяльність людей зі зміною дня і ночі, сезонів [4].

До основних одиниць вимірювання часу відносяться: *сторіччя, рік, місяць, доба, година, хвилина та секунда*.

Історично основною одиницею для вимірювання середніх інтервалів часу була ***доба*** (часто кажуть «день»), що вираховується з мінімальним повним циклів зміни сонячної освітленості (день і ніч). У результаті ділення доби на менші часові інтервали однакової довжини виникли години, хвилини і секунди. Походження поділу, ймовірно, пов'язано з дванадцятковою системою числення, якої дотримувалися в стародавньому Шумері. Добу ділили на два рівних послідовних інтервали (умовно день і ніч). Кожен із них ділили на 12 годин. Подальший поділ годин сходить до шістдесяткової системи числення. Кожну годину ділили на 60 хвилин, а кожну хвилину — на 60 секунд. Таким чином, у годині 3600 секунд; у добі — 24 години, або 1440 хвилин, або 86 400 секунд. Зараз саме ці одиниці найчастіше використовують для вимірювання та вираження проміжків часу[4].

> ***Секунда*** *(укр. позначення: с; міжнародне: s) є однією із семи основних одиниць у Міжнародній системі одиниць (SI) і однієї з трьох основних одиниць у системі СГС [4].*
>
> *Одиниці «**хвилина**» (укр. позначення: хв; міжнародне: min), «**година**» (укр. позначення: г; міжнародне: h) і «**доба**» (укр. позначення: д; міжнародне: d) не входять в систему SI, однак в Україні вони допущені для використання як позасистемні одиниці без обмеження терміну дії допуску, з областю застосування «усі області» [4].*

Основними засобами вимірювання є: календар та годинник. Найпоширенішим календарем, який використовується в усьому світі, і який використовується в західному світі, є Григоріанський календар, запроваджений Папою Римським Григорієм XII у 1582 році [2].

Це сонячний календар, дати в якому визначаються положенням Землі, що обертається навколо Сонця, на відміну від місячного календаря, який базується на русі Місяця. Григоріанський календар по суті виправив деякі помилки, притаманні юліанському календареві, який використовувався в Стародавньому Римі. Інші календарі, що використовуються в усьому світі, включають ісламський, китайський та єврейський календарі. Одна й та сама дата в часі буде описана по-різному залежно від календаря, що використовується. Розглянемо наступні приклади, кожен з яких показує один і той самий день (*рис. 21.2*) [4].

Григоріанський календар	*1 травня 2015*
Юліанський календар	*18 квітня 2015*
Ісламський календар	*12 раджаб 1436*
Індійський національний Шалівахана	*1937*
Єврейський календар	*12-й ліяр 5775*

Рисунок 21.2. Приклади написання однієї дати у різних календарях світу.

В зв'язку з тим що Григоріанський календар є найпоширенішим та прийнятий для літочислення практично у всьому світі, далі для проведення темпорального аналізу ми будемо використовувати саме його.

> *Слід зазначити, що запис дати в межах одного календаря також може відрізнятися.*

В Європі прийнято записувати дату у форматі *день-місяць-рік*, тоді як в інших країнах, наприклад, у США, прийнято використовувати *місяць-день-рік*. Ці відмінності не створюють особливих проблем в інтерпретації, якщо місяць написаний у текстовій формі: 1 травня 2015 року або травня 1 2015 року, та будуть сприйматися як однакові дати. Однак, якщо для позначення дати використовуються цифри, може виникнути плутанина [2; 5].

> *В Європі дата 01/05/2015 означає 1 травня 2015 року, проте в США вона буде сприйнята як 5 січня 2015 року. Якщо ви використовуєте дані з міжнародних джерел, важливо знати, в якому форматі подано дати. Це також може спричинити плутанину у використанні програмного забезпечення.*
>
> *Наприклад, ви використовуєте європейський формат, але ваше програмне забезпечення може використовувати американський формат. Більшість програм мають налаштування для адаптації до формату дати, але вам доведеться вручну налаштувати свої параметри, якщо ви використовуєте дані з різних країн.*

Вищезгадане питання стосується запису та передачі конкретних дат. У більшості випадків темпоральний аналіз проводиться з використанням програмного забезпечення обчислення та побудови графіків аналізу часу. У програмах зазвичай використовують інший формат для зберігання інформації про дати, ніж той, що використовується для запису або введення даних.

> ***Наприклад**, Microsoft Excel для Windows зберігає дату 1 травня 2015 року як 42125 – кожне ціле число вимірює кількість днів від початку січня 1900 року. Якби ми захотіли підрахувати кількість днів між 27 грудня 2014 року та 1 травня 2015 року, вручну це було б відносно складно. Windows Excel зберігає останню дату як 42000, тому в цьому випадку ми можемо легко обчислити розрив у 125 днів (42000-42125).*

Додаткової складності додає те, що не всі програми використовують однаковий формат дати – Microsoft Excel для комп'ютерів Macbook записує дату як кількість днів, що минули з початку січня 1904 року [4].

> *На фіксацію часу впливають різні системи обліку.*

Так, суттєвої різниці зазнав запис часу у США та Європейських країнах. Так, в США два періоди по 12 годин позначаються як AM (перед меридіаном) і PM (після меридіана). Ці періоди отримали свої назви від положення сонця по відношенню до середини небосхилу (меридіану). Аналогові годинники записують час у цих блоках по 12 годин, і ми всі добре знайомі з тим, як протікає час за цією системою вимірювання: кожен день починається опівночі або о 12:00, друга година дня починається о 1:00, полудень (або полудень) настає о 12:00, а день закінчується об 23:59 (або о 23:59:59, якщо вимірювати з точністю до секунд) [2].

Дещо інша система обліку часу використовується в Європі, де використовується 24-часовий годинник. За цим годинником години в добі вимірюються від 0 до 23. Доба починається о 00:00, половина доби – о 12:00, а закінчується о 23:59. Отже, 06:15 PM за 12-годинним годинником – це 18:15 за 24-годинним годинником [6]. Дату і час традиційно вимірювали окремо, користуючись різними інструментами календаря і годинника.

Коли ми хочемо проаналізувати часову інформацію, нас зазвичай цікавить точний час або комбінація дати і часу разом. Коли ми вводимо дані про дату або час у програму, вони, як правило, перетворюються у формат, який програма може використовувати для виконання обчислень та інших функцій. Як ми бачили раніше, Excel для Windows записує дати як кількість днів, що минули з початку січня 1900 року. Час у будь-якій даті записується у вигляді десяткового дробу від цього числа, тобто 12:00 вечора буде 0,5. Excel зберігає всю інформацію про дату/час в однаковому форматі, при цьому якщо вводити дату без часу, то за замовчуванням вказується час 12:00, а часу без дати присвоюється міфічна дата 00 січня 1900 року.

На *рис. 21.3* показано, як на програмному рівні записується різна інформація про дату і час в Microsoft Excel (дати подано в європейському форматі дд/мм/ррр).

Дата (дд/мм/рррр)	Час (24-часовий годинник гг:мм)	Дата/Час (дд/мм/рррр гг:мм)	Формат Microsoft Excel Windows
01/05/2015		01/05/2015 00:00	42125
01/06/2015		01/06/2015 00:00	42156
	12:00	00/01/1900 12:00	0.50000
	14:00	00/01/190014:00	058333
01/05/2015	14:00	01/05/2015 14:00	42125.58333
31/12/2014	23:59	31/12/2014 23:59	42004.99931
01/01/2015	00:00	01/01/2015 00:00	42005.00000

Рисунок 21.3. Приклади запису в програмному забезпечені Microsoft Excel різної інформації про дату і час [2].

Інші програми можуть використовувати різні системи, але загальна методологія однакова. У той час як Excel підраховує кількість днів з певного моменту часу (використовуючи десяткові дроби для позначення часу), система UNIX записує кількість секунд, що минули з опівночі 1 січня 1970 року.

Аналітику дуже важливо знати всі ці особливості фіксації часу, особливо під час імпорту даних із одної системи вимірювання в іншу та при використанні різного програмного забезпечення.

> *Так, **наприклад**, в черговій частині відділу поліції збереження даних про кримінальні правопорушення відбуваються у реляційній базі даних Microsoft SQL. Аналітик робить запит цих даних, з метою завантаження їх в електронну таблицю Excel. Чергова частина записує дані в окрему базу даних, яка запитується окремим користувачем, після чого створюється текстовий файл даних і надсилається аналітику електронною поштою. Потім вона експортує обидва набори даних в ArcGIS, де вони геокодуються, перетворюються у шейп-файл і проводиться подальший аналіз [4].*

У цьому прикладі дані щодо дати і часу переводяться з одного формату в інший, і аналітик повинен знати, яким чином в кожній системі записуються дані і як вони змінюються. Будь-яка помилка у записі даних призведе до подальших помилкових висновків аналітика.

Метод аналізу фіксованого часу (хвилин, годин та доби) вчинення правопорушень (час доби / день тижня) [2].

Як зазначалося, кожна злочинна подія має певний фіксований час її вчинення. Припустимо, що відомо точний час вчинення кримінального правопорушення. Також припустимо, що типове кримінальне правопорушення триває довше, ніж одну секунда, і в будь-якому випадку зафіксовано лише годину і хвилину вчинення кримінального правопорушення.

Розділивши добу на певну кількість періодів і підрахувавши кількість кримінальних правопорушень, що сталися в кожному часовому періоді, можна отримати досить чітку картину того, коли відбуваються кримінальні правопорушення. На наведених діаграмах можна побачити як розподіляються кримінальні правопорушення в залежності від часу доби (*рис. 21.4, 21.5*) [2].

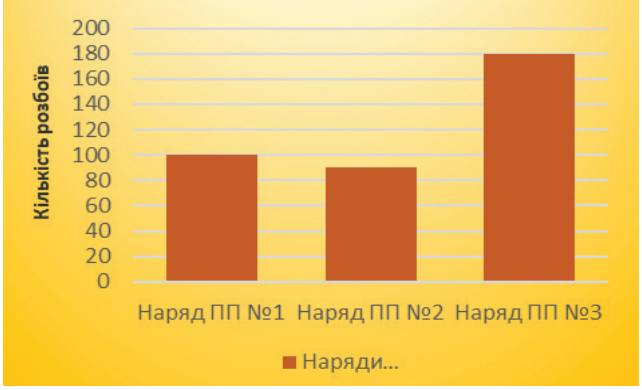
Крім цього можливо проаналізувати альтернативні залежності кількості правопорушень за часом доби. Так, наприклад, можливо зробити темпоральний аналіз на підставі встановлення залежності кількості кримінальних правопорушень від певних змін добових нарядів патрульної поліції, які чергують за встановленим графіком. Темпоральний аналіз даних взаємозв'язків можна проілюструвати у наступних діаграмах (*рис. 21.6*) [2]. Недоліком такого підходу є, по-перше, відсутність часової деталізації за добу, а по-друге, може вважатися спробою поставити у залежність активність злочинної діяльності від часу чергування конкретного наряду патрульного поліції. Тобто, під час роботи одних патрульних нарядів поліції певний вид кримінальних правопорушень збільшується, а під час роботи інших, навпаки – зменшується.



Рисунок 21.4. Діаграма погодинного розподілу кількості розбоїв за добу



Рисунок 21.5. Діаграма погодинного розподілу кількості грабежів за добу



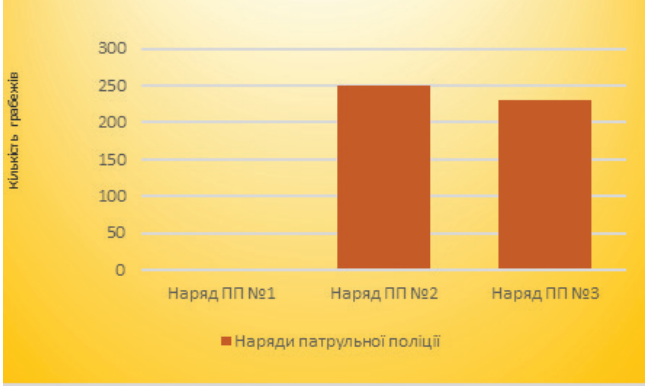
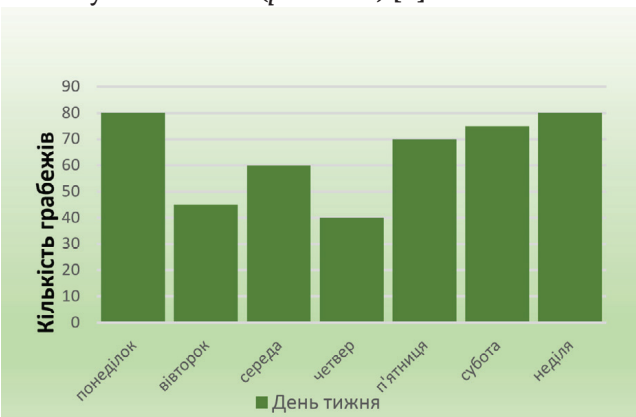


Рисунок 21.6. Діаграми зв'язку рівня розбоїв і грабежів з чергуванням певного наряду патрульної поліції у певний проміжок часу

Наведені вище діаграми використовуються під час вирішення питання, в який час (години, хвилини) були вчинені кримінальні правопорушення (розбої та грабежі). Але якщо необхідно встановити конкретну добу, в яку вчиняється кримінальне правопорушення. У цьому випадку можливо провести дуже схожий аналіз взаємозв'язку кількості кримінальних правопорушень від дня тижня, коли вони були вчинені (*рис. 21.7*) [2].



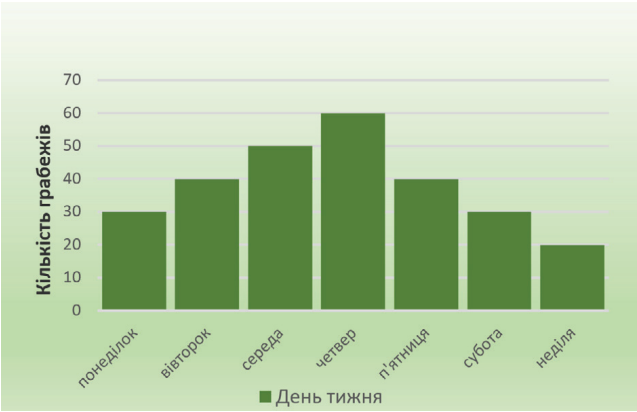


Рисунок 21.7. Діаграми зв'язку кількості розбоїв і грабежів з конкретним днем тижня

З метою представлення більш повної картини взаємозв'язку динаміки злочинної діяльності від часової ознаки за добу та денної за тиждень, необхідно об'єднати результати цих аналізів. У наведеній нижче матриці (*рис. 21.8*) представлені об'єднані дані за кількістю вчинених розбоїв за певну годину доби та день тижня. Під час аналізу було застосоване форматування в Excel, з метою більш швидкого визначення ключових проблемних часових рамок.

Після проведення зведеного темпорального аналізу, можна побачити тенденцію до вчинення розбоїв у певний час доби та дня тижня. Так, підвищення активності щодо вчинення розбоїв спостерігається у вихідні дні з 19:00 до 20:00, з 22:00 до 23:00 та з 01:00 до 02:00. Крім цього активність спостерігається в будні дні з 02:00 до 03:00, а також в п'ятницю та суботу з 13:00 до 16:00. Враховуючи місця де вчиняються ці розбої можна виділити дві групи: перша – в нічний та вечірній час (переважно у вихідні дні) біля барів та ресторанів, а друга – переважно в другій половині робочих днів в парках та скверах.

Зведена таблиця визначення кількості розбоїв за годинами доби та днями тижня								
Години/Дні	**понеділок**	**вівторок**	**середа**	**четвер**	**п'ятниця**	**субота**	**неділя**	**ВСЬОГО**
00	5	5			5		5	**20**
01	5		5	5		5	5	**25**
02	5	5	5	5		5	5	**30**
03		5	5		5	5	5	**25**
04	5	5	5		5		5	**25**
05	5							**5**
06							5	**5**
07								**0**
08	5				5			**10**
09			5			5	5	**15**
10	5			5		5		**15**
11			5		5			**10**
12		5		5		5	5	**20**
13	5	5	5		5	5		**25**
14	5		5	5	5	5		**25**
15	5	5	5	5	5	5		**30**
16	5	5	5		5	5	5	**30**
17			5	5		5	5	**20**
18	5		5	5	5		5	**25**
19	5				5	5	5	**20**
20					5	5	5	**15**
21	5						5	**10**
22	5				5	5	5	**20**
23	5	5			5	5	5	**25**
ВСЬОГО	**80**	**45**	**60**	**40**	**70**	**75**	**80**	**450**

Рисунок 21.8. Зведення визначення кількості розбоїв за годинами доби та днями тижня з визначенням червоним кольором дільниць підвищеної злочинної активності

Метод аналізу часових періодів (інтервалів) вчинення кримінальних правопорушень у серії [2; 4]**.**

Часові періоди та інтервали враховують однотипні події, що відбуваються на одній території, за якою проводиться аналіз. Існує три основні види часових періодів та інтервалів між кримінальними правопорушеннями:

- ***рівномірний*** *– кримінальні правопорушення вчиняються з однаковими інтервалами одне від одного;*
- ***кластерний*** *– кримінальні правопорушення вчиняються з найменшими інтервалами одне від одного;*
- ***випадковий*** *– тенденції щодо будь-якої системності у часових інтервалах між вчиненням кримінальних правопорушень не спостерігаються.*

Рівномірний часовий інтервал має місце тоді, коли кримінальні правопорушення вчиняються зі значними часовими інтервалами одне від одного. При цьому ці інтервали носять рівномірний характер.

Кластерний часовий інтервал – це коли кримінальні правопорушення мають тенденцію відбуватися близько одне від одного. Прикладом такого розподілу є квартирні крадіжки, коли об'єктом нападу послідовно стають різні квартири в одному комплексі, а після певного періоду бездіяльності злочинець переходить до інших комплексів [4].

Випадковий часовий інтервал не підходить до жодної з двох попередніх категорій. Він цілком може бути результатом поєднання кластерного та рівномірного видів часових інтервалів або справді може бути хаотичним [2].

При цьому у всіх видах часових інтервалів точно відома їх величина. Для кластерного виду – вона розраховується як час між середніми показниками сусідніх кластерів. Одиниці для визначення обираються будь-які: хвилини, години, дні, тижні, все залежить від поставлених завдань перед аналітиком. Аналіз групи часових інтервалів використовується для прогнозування настання кримінальних правопорушень у майбутньому.

Метод аналізу темпу (зміни динаміки) часових інтервалів між часом вчинення кримінальних правопорушень в одній серії [4].

У зв'язку з тим, що час рухається тільки в одному напрямку, при значній кількості часових періодів в серії кримінальних правопорушень, можливо провести порівняльний аналіз не тільки протяжності часових періодів, а і прослідкувати зміни у динаміці збільшення або зменшення протяжності часових періодів. Дана ознака називається темпом. Темп часових періодів може бути [4]:

- *прискорений* – протяжність часових інтервалів між кримінальними правопорушеннями зменшуються зі збільшенням кількості правопорушень;
- *уповільнений* – часовий інтервал між кримінальними правопорушеннями збільшується зі збільшенням кількості правопорушень;
- *стабільний* – часовий інтервал між кримінальними правопорушеннями не зазнає змін.

Метод аналізу активності правопорушника (злочинця) у певний часовий період [2].

Якщо є можливість спостерігати за злочинцем достатньо довгий період часу, можливо виявити періоди коли злочинець проявляє певну активність, яка може бути пов'язана саме з підготовкою або безпосереднім вчиненням кримінального правопорушення. Аналітик діючи в умовах невідомого, повинен проаналізувати активність злочинця протягом часового періоду (доба, тиждень, місяць), виявити певні закономірності та скласти графік (розклад) за аналогією складання графіку «годин в добі / днів у тижні» [7]. У подальшому аналітик може використати цю інформацію, щоб виявити часові періоди коли саме вчиняється кримінальне правопорушення або спрогнозувати коли воно може відбутися у майбутньому. Для цього кримінальний аналітик використовує різноманітну інформацію, отриману з доступних джерел: дані про вчинені кримінальні правопорушення, інформація про правопорушника отримана під час проведення негласних слідчих (розшукових) дій, банківські операції тощо.

Метод аналізу часових циклів та сезонності злочинної діяльності [2].

Злочинну активність правопорушника можливо встановити тільки при виявлені певних закономірностей у його поведінці, пов'язаних з конкретними часовими періодами. Якщо аналітик спостерігає тенденцію до повторювання один і тих самих дій у певний час, неважливо, це певні дні тижня, певні місяці чи пора року, можливим є виявлення часових або сезонних циклів у злочинній діяльності [8]. Часові цикли злочинної діяльності є основою для прогнозування відповідних ризиків у майбутньому та прийняття рішень щодо їх усунення або мінімізації.

Наприклад, поліцією було виявлено низку випадків пошкодження невідомими особами транспортних засобів, які знаходилися в одному мікрорайоні міста [2]. Темпоральний аналіз цих кримінальних правопорушень показав, що між вчиненням цих кримінальних правопорушень рівномірний часовий інтервал у 14 діб, а повідомлення в поліцію надходять ввечері кожного другого четверга місяця. Ця інформація стала підставою для пошуку та виявлення правопорушників, шляхом посилення нарядів патрульної поліції у вечірній час кожного другого четверга місяця. У результаті чого у цей часовий період була затримана група молодих чоловіків, які працювали у приватній установі. Дана установа відкрилася нещодавно і керівництвом установи було встановлено виплату заробітної плати своїм працівникам саме у четвер, один раз на два тижні. Тому група молодих чоловіків саме в цей час святкували отримання заробітної плати в місцевому барі, а по дорозі додому продовжували «святкування», розтрощуючи припарковані автомобілі.

Метод темпорального аналізу в умовах відсутності даних щодо часу вчинення кримінального правопорушення [2; 9].

Вище розглядалися методи темпорального аналізу, при яких була відома інформація про час вчинення кримінального правопорушення, часові періоди (інтервали) між кримінальними правопорушеннями в одній серії, інші часові показники, пов'язані з життєдіяльністю кримінального правопорушника (злочинця). Але це буває не завжди. Так, наприклад, результати аналізу серії грабежів на підставі інформації отриманої у час повідомлення про злочин може суттєво розходитися з результатами аналізу на підставі інформації коли дійсно був вчинений злочин. Це пов'язано, перш за все з тим, що потерпілі не завжди одразу повідомляють в поліцію про факт кримінального правопорушення. Потерпілий може очікувати кілька днів допоки прийме рішення і зателефонує до відділу поліції або відвідає його особисто. У таких ситуаціях рекомендується використовувати метод, відомий як аористичний аналіз.

Аористичний аналіз. Цей метод темпорального аналізу базується на встановленні ймовірності вчинення кримінального правопорушення у певний час. Наприклад, відомо, що пограбування відбулося рівно о 14:30. У цьому випадку ми говоримо, що ймовірність того, що злочин стався між 14:00 та 15:00, дорівнює 100%. В іншому випадку відомо, що людина вийшла з дому о 8 ранку на роботу й повернулася додому о 18:00 та виявила у цей час, що її квартиру пограбували. У цьому випадку

відомо, що злочин стався в певний час між 8 ранку і 6 вечора, але не можливо точно знати, коли саме. Цей злочин міг статися в будь-який з 10 годин між тим, як потерпілий вийшов з дому і повернувся з роботи. Ймовірність того, що цей злочин стався, наприклад, між 14:00 та 15:00, становить 10%, так само як і ймовірність того, що він стався в будь-який інший період перебування поза квартирою[9].

Для будь-якого набору даних ризик вчинення злочину в будь-який період дорівнює сумі всіх оцінок ймовірності для кожного періоду. Якщо взяти за часовий цикл тиждень, то матимемо 168 періодів тривалістю 1 година, протягом яких може статися злочин [2]. Якщо сім'я повернулася додому з тижневої відпустки і виявила, що їхній будинок пограбували, ймовірність того, що злочин стався в будь-яку з годин тижня, становить лише 0,6%. Низька ймовірність для кожної години означає, що цей злочин не матиме значного впливу при часовому аналізі сукупності квартирних крадіжок – так і має бути, оскільки ми маємо дуже малу часову визначеність щодо злочину.

Проведення аористичного аналізу такого типу спочатку може показатися досить складним. На практиці аналітики розробляють матрицю (шаблон), який можна повторно використовувати з будь-яким майбутнім набором даних.

Методи аналізу часових рядів (прогнозування) [4].

Прогнозування – це те, чого більшість аналітиків очікують від темпорального аналізу. Кінцевою метою будь-якої роботи є повне розуміння того, що сталося в минулому, з метою передбачення того, що станеться в майбутньому. Прогнозування під час стратегічного аналізу є більш ефективним ніж при тактичному. Так, виявити часову циклічність, наприклад, у сезонних крадіжках та спрогнозувати її в майбутньому не так складно, як, наприклад, спрогнозувати день та час наступного вчинення злочинцем правопорушення. Це пов'язано, перш за все, з протяжністю часового періоду – на довгострокових періодах імовірність помилки значно менша, а по-друге, із наявністю інших обставин у прогнозуванні злочинної діяльності конкретної особи, у тому числі непередбачуваних, які можуть збільшити або зменшити вірогідність прогнозу.

Види методів аналізу часових рядів (прогнозування) [4]:
- *лінійні прогнози;*
- *циклічні прогнози;*
- *прогнози провідних індикаторів.*

Лінійні прогнози. Лінійні прогнози екстраполюють те, що станеться, на основі тенденцій у минулому. Для візуалізації таких тенденцій і складання прогнозу можна використовувати темпограму, яка генерує лінію тренду на основі аналізу інтервалу між подіями. Більшість програм, які використовуються для побудови графіків часових даних, можуть додавати таку лінію тренду. Лінію можна екстраполювати за межі останньої відомої точки даних, щоб оцінити, коли відбудеться наступна подія – це можна зробити візуально на графіку або за допомогою математичної функції, яка описує лінію тренду. Також метод лінійного прогнозу можна застосовувати на часових періодах (інтервалах), що змінюють темп.

Циклічні прогнози. Описані раніше сезонні моделі є дуже простим прикладом циклічного тренду, на якому можна будувати стратегічні прогнози. Часова матриця, яка визначає «час доби / день тижня», також може описувати циклічну тенденцію. Щоб перевірити, чи існує такий цикл, можна використати графік цих подій – сам графік може бути важко інтерпретувати візуально як інструмент звітності, але аналітик може використовувати його, щоб підтвердити, чи повторюється патерн, описаний у часовій матриці, тиждень за тижнем. Якщо так, то часову матрицю можна використовувати для прогнозування майбутніх кримінальних правопорушень.

Прогнози провідних індикаторів. Цей тип прогнозування є дво- або багатоваріантним за своєю природою. Застосування цього методу передбачає використання різних факторів та обставин у поєднанні з часовими елементами структури кримінального правопорушення. Ці фактори або обставини слугують індикаторами, за якими в подальшому будується лінія тренду. Так, наприклад, якщо відомо що є серія крадіжок, які вчиняються наркозалежним. Відома вартість майна викраденого в кожному конкретному випадку. Але невідомий конкретний час вчинення правопорушень. У цій ситуації можливим є застосування методу прогнозу провідних індикаторів та використання в якості такого індикатору – вартості викраденого майна. Далі побудувавши діаграму взаємозв'язку вартості викраденого майна до інтервалів між злочинами, можна отримати горизонтальну лінію тренду. Це дасть нам можливість визначити кількість днів, на протязі яких наркозалежний злочинець витратить вкрадені кошти та спрогнозувати коли буде вчинена наступна крадіжка.

МЕТОДИ ЧАСОПРОСТОРОВОГО АНАЛІЗУ

Злочинність рідко буває випадковою або рівномірно розподіленою у просторі; наприклад, в одних районах більше кримінальних правопорушень, ніж в інших, також види кримінальних правопорушень, що вчиняються в одних районах, відрізняються від інших. Виявлення районів з високим рівнем злочинності, або як їх називають «гарячих точок», відіграє ключову роль у роботі правоохоронних органів та протидії злочинності на проблемних територіях [4]. У стратегічних цілях і для вирішення проблем виявлення районів з високим рівнем злочинності може бути корисним для розробки та оцінки заходів реагування поліції, а також для тестування на предмет просторового переміщення або розповсюдження переваг. У тактичних цілях аналіз «гарячих точок» може сигналізувати про наявність моделі злочинності та допомогти правоохоронним органам краще визначати пріоритети і розподіляти ресурси на конкретні напрями. Таким чином, в основі аналізу злочинності лежить підтримка та надання необхідної інформації для запобігання, реагування або розслідування кримінальних правопорушень.

Перед аналітиками стоїть ряд завдань, таких як об'єктивне виявлення зон з високим рівнем злочинності, ефективна ілюстрація цих зон на карті, а також допомога в розумінні того, як розвиваються і зберігаються зони з високим рівнем злочинності (проблемні зони). Для цього аналітик повинен розуміти деякі з наявних методів і послідовно намагатися їх використовувати. Існує багато методів виявлення гарячих точок. Кожен з них має свої сильні та слабкі сторони і може бути придатним для однієї області, але не для іншої. Незалежно від обраного методу, він повинен бути обґрунтований як емпірично, так і теоретично. Ці методи, як правило, включають розробку карт злочинності та застосування статистичних тестів для визначення наявності просторової кластеризації.

Аналітичні методи, що використовуються з картами злочинності, включають [9]:

- *ручний аналіз;*
- *аналіз в нечіткому режимі;*
- *аналіз градуйованої кольорової карти або карти Хороплету,*
- *аналіз стандартного відхилення;*
- *картографування комірок сітки або аналіз щільності.*

Більшість з цих методів буде розглянуто у розділі «Геопросторовий аналіз», у зв'язку з тим що методи просторового аналізу напряму пов'язані з картографуваннями та аналізом карт злочинності та не можуть розглядатися окремо. Але є методи які частково пов'язані з картографуванням і їх необхідно розглянути саме в даному розділі.

Метод моделювання ризиків на місцевості.

Метод моделювання ризиків на місцевості (*англійською абревіатура – RTM*) був розроблений у 2009 році Джоелом Капланом і Леслі Кеннеді, щоб використовувати дані з різних джерел і застосовувати легкодоступні методи, які могли б повторити інші люди. Щоб зробити його більш доступним для людей з обмеженими здібностями до ГІС і статистики, Ратгерський університет у 2013 році допоміг розробити RTMDx Utility – безкоштовну програму, яка автоматизує RTM [10].

Особливості ландшафту можуть впливати на поведінку та сприяти їй. Розглянемо місце, де постійно граються діти. Якщо відійти від уваги до скупчення дітей, можна помітити, що там, де вони граються, є гойдалки, гірки та відкриті поля. Ці особливості місця приваблюють дітей саме туди, а не в інші місця, де немає таких розважальних якостей. Подібним чином просторові фактори можуть впливати на серйозність і тривалість проблем зі злочинністю. Моделювання ландшафту ризиків полягає у визначенні ризиків, пов'язаних з особливостями ландшафту, та моделюванням того, як вони поєднуються для створення унікальних поведінкових умов для кримінальних правопорушень.

Завдяки науковим дослідженням було з'ясовано, що ризики, які проявляються у специфічних особливостях ландшафту, та ефекти їхньої взаємодії можуть бути використані для обчислення ймовірності злочинної поведінки. RTM створює цю комплексну модель просторової вразливості до злочинів на мікрорівні.

Процес RTM починається з відбору та зважування факторів, які географічно пов'язані зі злочинними інцидентами. Потім створюється остаточна модель, яка, по суті, «малює картину» місць, де злочинна поведінка є статистично найбільш вірогідною [10].

За всіма намірами і цілями RTM є діагностичним методом. Діагностуючи природні кореляти певної поведінки або результатів, ви можете робити дуже точні прогнози. Знаючи просторові фактори ризику, можна розробити заходи втручання, щоб протидіяти злочинності у короткостроковій перспективі і зменшити фактори ризику на цих територіях, щоб вони стали менш привабливими для злочинців у довгостроковій перспективі. За допомогою RTM можливо визначити пріоритети факторів ризику і призначити заходи для їх пом'якшення, навіть в умовах обмежених ресурсів. Було доведено, що RTM робить це для різних типів кримінальних правопорушень у різних умовах.

«Гарячі точки» вказують на те, де скупчується злочинність, але не обов'язково на те, чому. Занадто часто люди зосереджуються на гарячих точках, не приділяючи належної уваги просторовим характеристикам, які роблять ці райони менш привабливими для життя. Хоча існують соціальні, ситуативні, політичні, культурні та інші фактори, пов'язані з різноманітними наслідками злочинності, існує також і просторовий компонент. «Гарячі точки» – це лише ознаки та симптоми місць, які є дуже сприятливими для вчинення злочинів. RTM просувається в цьому напрямі, надаючи просторову діагностику [10].

Потенціал візуальної комунікації карт ризикованих територій і пов'язаних з ними просторових даних практично не обмежений. Переглядаючи карту ризикованих територій у GIS, можливо коригувати умовні позначення та створювати остаточні макети карт для візуальної комунікації просторових вразливостей певної території. Растрові карти на мікрорівні можна створювати і представляти у вигляді зображень у звітах. Комірки растрової карти можна також об'єднувати за допомогою просторових з'єднань з сегментами вулиць, поліцейськими ділянками, переписними дільницями і так далі. Карти можна навіть експортувати у форматі KML і накладати на них шари в Google.

Утиліта Risk Terrain Modeling Diagnostics (RTMDx) – це програмне забезпечення для RTM і для діагностики просторової вразливості до злочинності [10]. Вона допомагає виявляти та повідомляти про фактори протиправної поведінки та злочинні інциденти. Інформаційні продукти можуть бути використані для прогнозування місць, які будуть найбільш вірогідними для злочинної діяльності, визначення місць виникнення або скупчення нових злочинних інцидентів, розробки заходів, орієнтованих на конкретні місця, стратегічного і тактичного розподілу ресурсів, а також визначення пріоритетності зусиль щодо зниження ризиків злочинності.

RTMDx автоматизує більшість етапів RTM. Алгоритм емпірично тестує різноманітні просторові впливи та кроки аналізу для кожного вхідного фактору ризику, щоб визначити найбільш емпірично та теоретично обґрунтовані просторові асоціації з відомими місцями вчинення кримінальних правопорушень. Потім відбираються лише найбільш підходящі фактори ризику (з оптимально врахованими просторовими впливами) для створення «найкращої» моделі ризиків у просторі [10]. Остаточна модель відображає вразливість до злочинів з відносними показниками ризику в кожному місці досліджуваної території. Фактори навколишнього середовища, які створюють конкретні фактори вразливості в певних місцях, перераховуються і зважуються відповідно до їх відносного просторового впливу на кінцеву подію. Це допомагає визначити пріоритетність заходів зі зниження ризиків.

Роль, яку може відігравати RTM, випливає із запиту архівних даних і даних у реальному часі для отримання картини злочинності. Ця інформація може бути важливою в управлінні організацією таким чином, щоб рішення про протидію злочинності відповідали дійсності, перевірялися на практиці та були ефективними.

Метод «шлях до місця злочину» [4; 11]

Це аналітичний метод, який оцінює ймовірне місце життєдіяльності (місця відпочинку, місце безпосереднього проживання, місце роботи, місця зустрічі з родичами, друзями тощо) кримінального правопорушника, зазвичай того, хто вчинив кілька пов'язаних між собою кримінальних правопорушень. Він ґрунтується на більш загальній теорії місцезнаходження, яка намагається знайти оптимальне місце для будь-якого конкретного розподілу діяльності, населення або подій у регіоні.

Згідно з передумовою, що лежить в основі концепції методу «шляху до місця злочину», люди вчиняють злочини в рамках своєї повсякденної діяльності. Місця вчинення злочинів будуть відносно близькими до місць, де правопорушник працює, спить і займається побутовими справами. Це узгоджується з теорією повсякденної діяльності Коена і Фелсона, яка стверджує, що будь-який насильницький злочин відбувається під час повсякденної діяльності жертви і злочинця [11]. Злочин можливий лише на їх перетині в часі та просторі, коли відсутній ефективний контроль за безпекою потенційної жертви.

Одним із прикладів застосування методу «шлях до місця злочину» у практиці кримінального аналізу є географічне профілювання. Цей процес, відомий як геопрофілювання, був розроблений на початку 1990-х років доктором Кімом Россмо в рамках його докторського дослідження в Університеті Саймона Фрейзера. Россмо заснував компанію Environmental Criminology Research Inc., яка створила і запатентувала технологію для автоматизації процесу геопрофілювання [11]. Геопрофіль будується шляхом аналізу відомих місць інцидентів, які географічно пов'язані з невідомою базою операцій, з метою визначення, де ця база, найімовірніше, знаходиться.

Хоча геопрофілювання не обмежується насильницькими злочинами, воно зазвичай використовується для інцидентів, пов'язаних біологічними доказами або способом вчинення злочину, таких як серія сексуальних нападів. Геопрофіль зображується на растровій карті ймовірності (*тепловій*

карті), яка показує ймовірність знаходження місця проживання в кожній комірці сітки за кольором (від холодного до гарячого).

Слід зазначити, що модель ґрунтується на концепції, що кримінальний правопорушник має одне стабільне місце проживання, з якого він вирушає на пошуки підходящих жертв, або рухаючись з якого він стикається з жертвами впродовж свого звичайного дня. Цей метод не є ефективним для виявлення кримінальних правопорушників, які знаходять жертв в Інтернеті, за допомогою друкованих оголошень або некрологів, або під час подорожей за межами своєї місцевості (наприклад, водії далекобійники, бродяги) [4]. Кілька компаній-розробників програмного забезпечення для аналізу кримінальних правопорушень вже вбудували цю технологію у свої продукти для використання під час розслідувань серійних злочинів з метою виявлення потенційних жертв.

Таким чином, час вчинення злочину відіграє важливу роль у розслідуванні кримінальних правопорушень. Але він є не тільки предметом доказування, а й дієвим засобом отримання нової доказової або оперативно-розшукової інформації. Аналіз часових періодів або конкретного часу в якому перебуває об'єкт дослідження дозволяє встановити взаємозв'язок між особою правопорушника, особою потерпілого та місцем вчинення правопорушення, іноді визначити спосіб вчинення правопорушення. Застосування темпорального аналізу, як у розслідуванні кримінальних правопорушень, так й при оцінці загроз злочинності, значно підвищує ефективність діяльності правоохоронних органів у протидії злочинності.

Застосовувати темпоральний аналіз можливо як на стратегічному, так й на тактичному рівнях. Так, за допомогою методів темпорального аналізу **на стратегічному рівні** можливо вирішити наступні завдання:

оцінити загрозу вчинення певного виду злочину у наступному періоді;

визначити сили та засоби необхідні для протидії певному виду злочину у наступному періоді;

визначити причини зниження рівня розслідування певного виду злочину за певний період тощо.

На тактичному рівні –

підготовка рекомендацій, щодо попередження певного виду злочину;

складання плану ефективного застосування сил та засобів під час попередження та розслідування певного виду злочину на певній місцевості тощо.

Однак, треба пам'ятати, що при проведенні темпорального аналізу, час необхідно розглядати у сукупності з іншими елементами та чинниками злочинної діяльності (геопросторовими, поведінковими, історичними, культурними тощо). Так, розглянуті методи моделювання ризиків на місцевості та «шлях до місця злочину» вказують саме на такий дієвий симбіоз цих елементів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Кримінальний процесуальний кодекс України: Кодекс України; Закон, Кодекс від 13 квіт. 2012 р. № 4651-VI. URL: http://zakon1.rada.gov.ua
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. Timothy C., Hart (2021). Investigating Crime Pattern Stability at Micro-Temporal Intervals: Implications for Crime Analysis and Hotspot Policing Strategies. *Criminal Justice Review*, 46 (2), 173-189.
4. International Association of Crime Analysts (2011). *Crime pattern definitions for tactical analysis.* Overland Park.
5. Тактичний кримінальний аналіз: теорія та практика; навчальний посібник / О.Є. Користін, Н.П. Свиридюк, О.М. Цільмак, О.М. Заєць, К.Ю. Ісмайлов, В.А. Некрасов. Одеса: РВВ ОДУВС, 2019. 179 с.
6. Groff, E.R., & Taniguchi, T. (2018). *Micro-level policing for preventing near repeat residential burglary*: Final monograph. Police Foundation.
7. Chainey, S., Tompson, L. & Uhlig, S. (2008). The utility of hotspot mapping for predicting spatial patterns of crime. *Security Journal*, 21 (1), 4–28. DOI: 10.1057/palgrave.sj.8350066
8. Perry, W.L., McInnis, B., Price, C.C., Smith, S.C., & Hollywood, J.S. (2013). *Predictive policing: The role of crime forecasting in law enforcement operations*. Rand Corporation. Pitney Bowes Software (2016). MapInfo professional. Pitney Bowes.
9. Epifanio, Pecharromán (2016). Crime Predictive Analysis Based on Geo-intelligence. *The International Journal of Intelligence, Security, and Public Affairs*, 18:3, 221-248.
10. 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.
11. Felson, M. & Eckert, M. (2019). Crime and everyday life: A brief introduction (6th ed.). Sage. Fielding, M., & Jones, V. (2011). Disrupting the optimal forager: Predictive risk mapping and domestic burglary reduction in Trafford. Greater Manchester. *International Journal of Police Science & Management*, 14 (1), 30–41.

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].

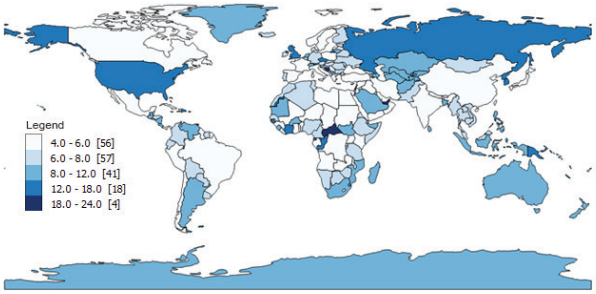


Рисунок 22.1. Хороплетна карта світу з використанням методу природних розривів.

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].

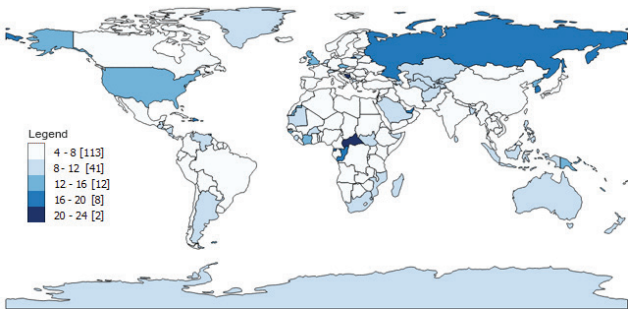


Рисунок 22.2. Хороплетна карта світу з використанням методу рівних інтервалів.

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].

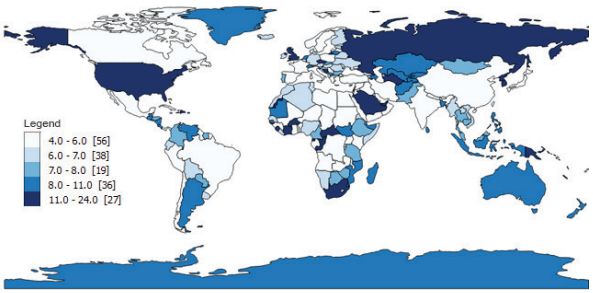


Рисунок 22.3. Хороплетна карта світу з використанням методу квантилів.

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*).

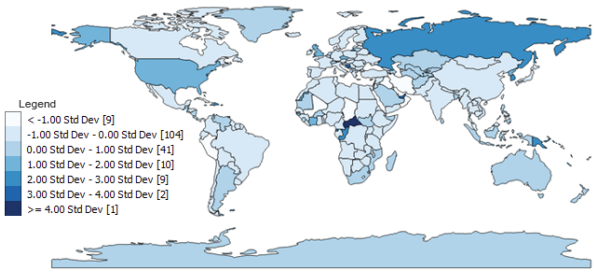


Рисунок 22.4. Хороплетна карта світу з використанням методу стандартних відхилень.

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*).

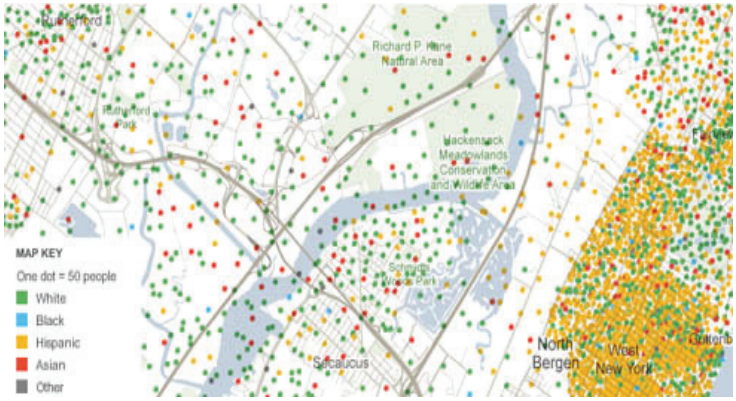


Рисунок 22.6. Картографування методом крапок на прикладі карти із зображенням крапками розселення представників різних етнічних груп (зображення з сайту www.danieljlewis.org)

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*).

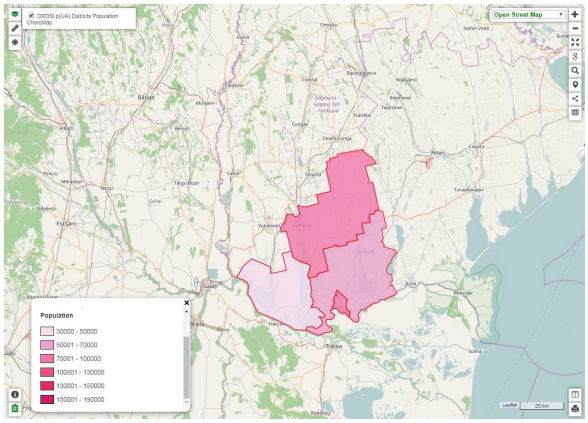


Рисунок 22.7. Картографування методом Хороплету на прикладі кількості населення у районах Дунайського регіону України

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*).

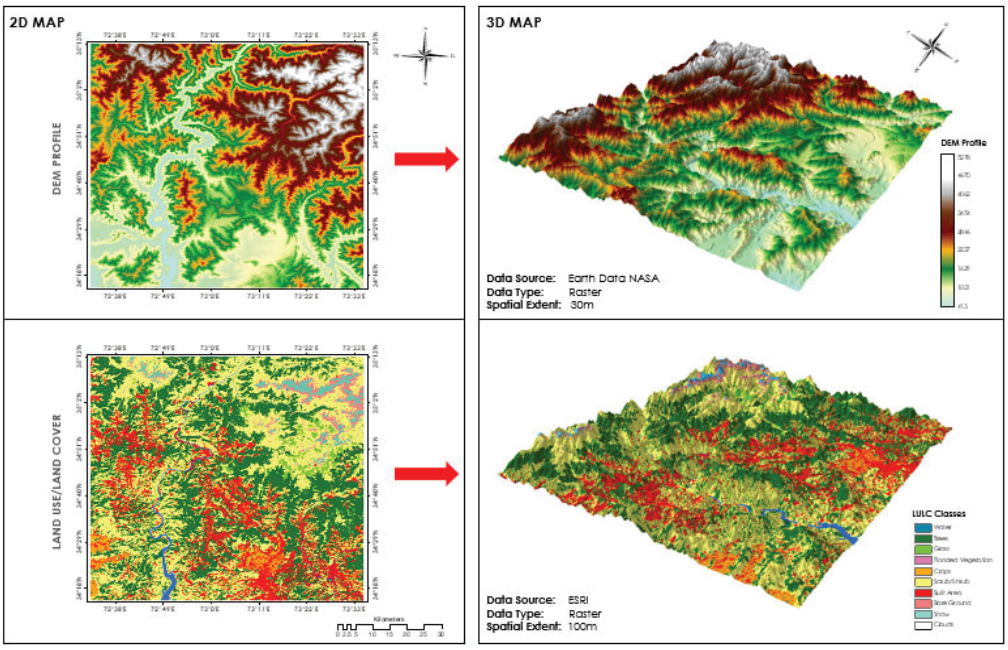


Рисунок 22.8. Приклад використання методу просторового аналізу на квадратній області географічної карти

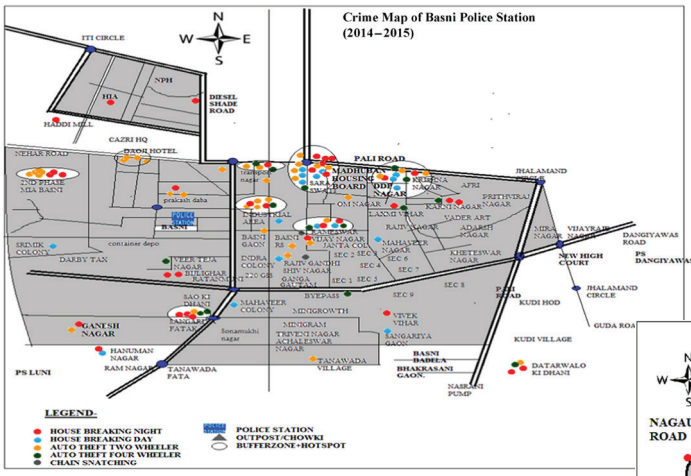


Рисунок 22.9. Карта злочинності Баснінського відділу поліції (2014–2015)

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]:

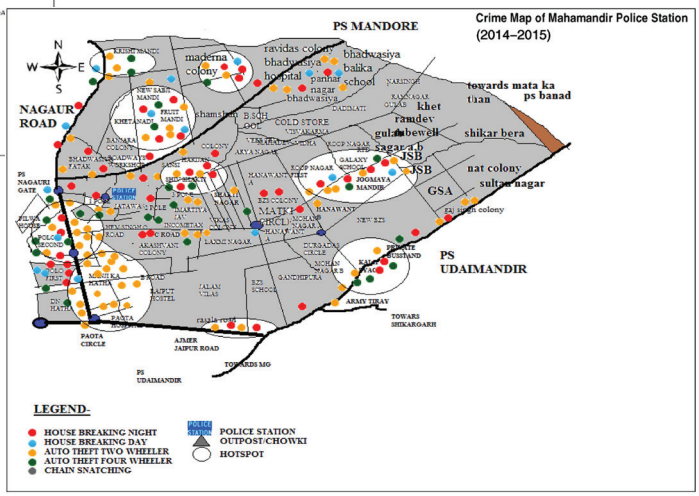


Рисунок 22.10. Карта злочинності відділу поліції Махамандір (2014–2015)

- ✓ *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].

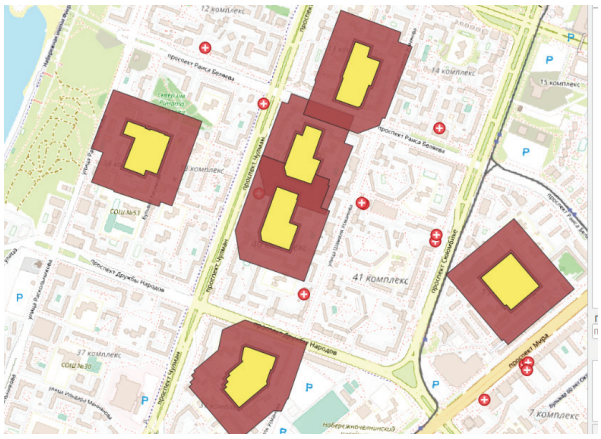


Рисунок 22. 11. Використання методу буферизації на прикладі відображення школи у вигляді багатокутника з прилягаючою територією

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].

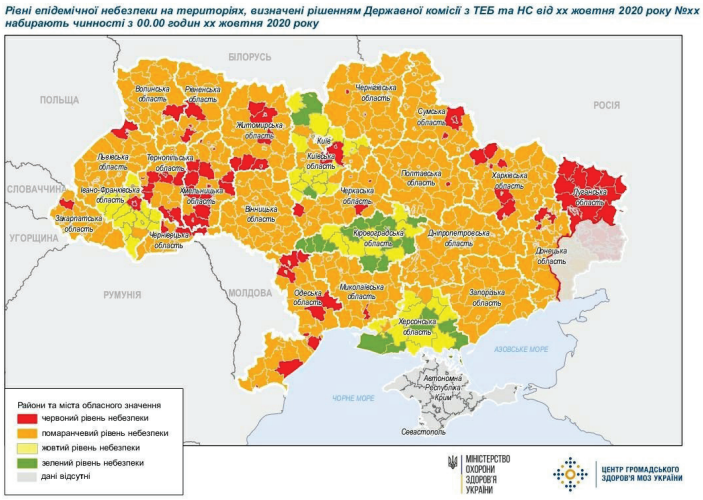
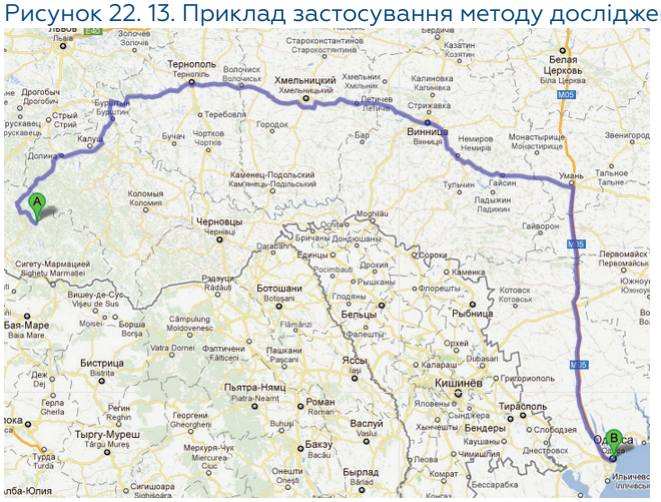


Рисунок 22.12. Приклад застосування методу зонального дослідження (аналізу) об'єктів на карті

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.*

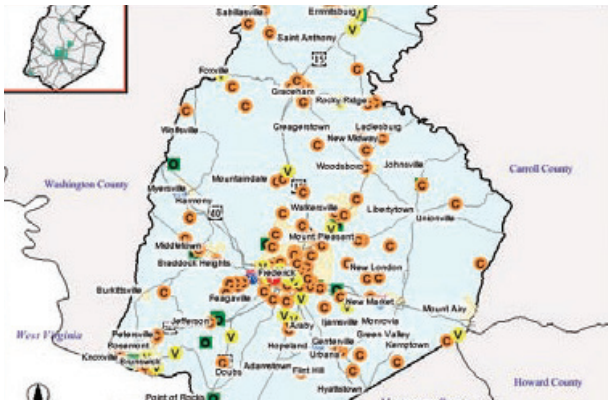
Ретроспективний аналіз

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.

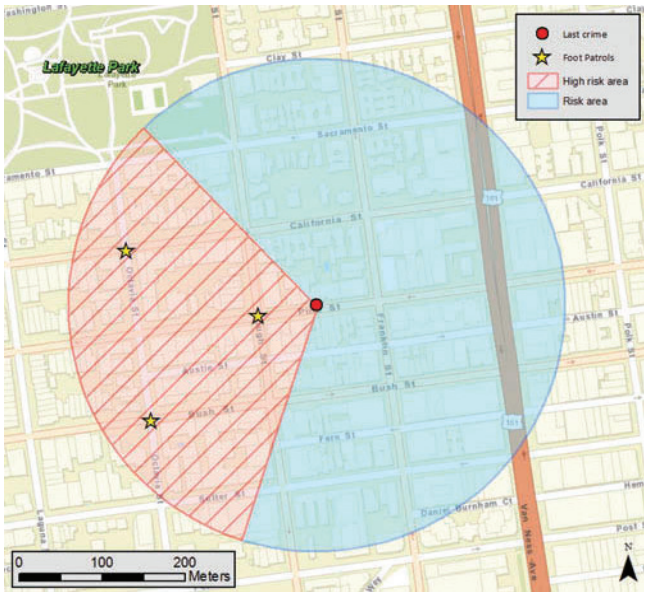


Аналіз гарячих точок є відправною точкою якісного аналізу карти злочинності. На основі аналізу великої кількості даних, аналіз гарячих точок слід використовувати для прогнозування областей підвищеного ризику злочинності на основі злочинів минулих років для вирішення проблем та відповідного планування 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].

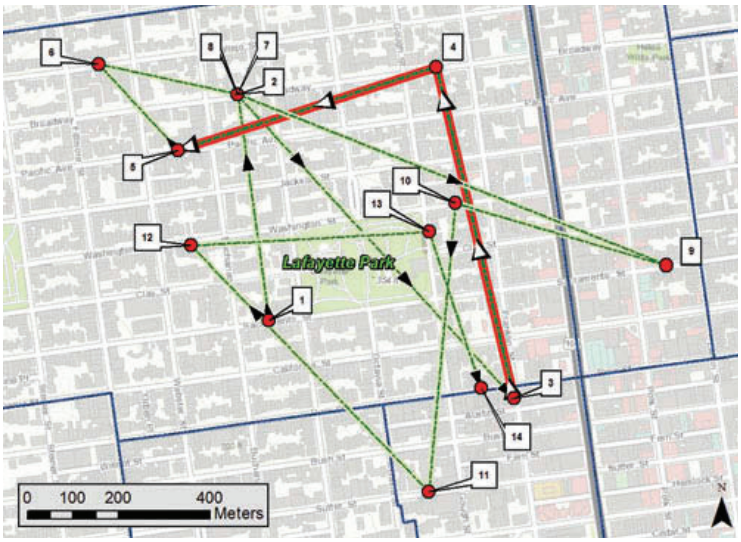


Рисунок 22. 16. Приклад застосування методу просторового аналізу при картографуванні місць вчинення квартирних крадіжок (помічені червоними крапками) в результаті чого аналітиком була виявлена закономірність руху за годинниковою стрілкою коло парку

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]*

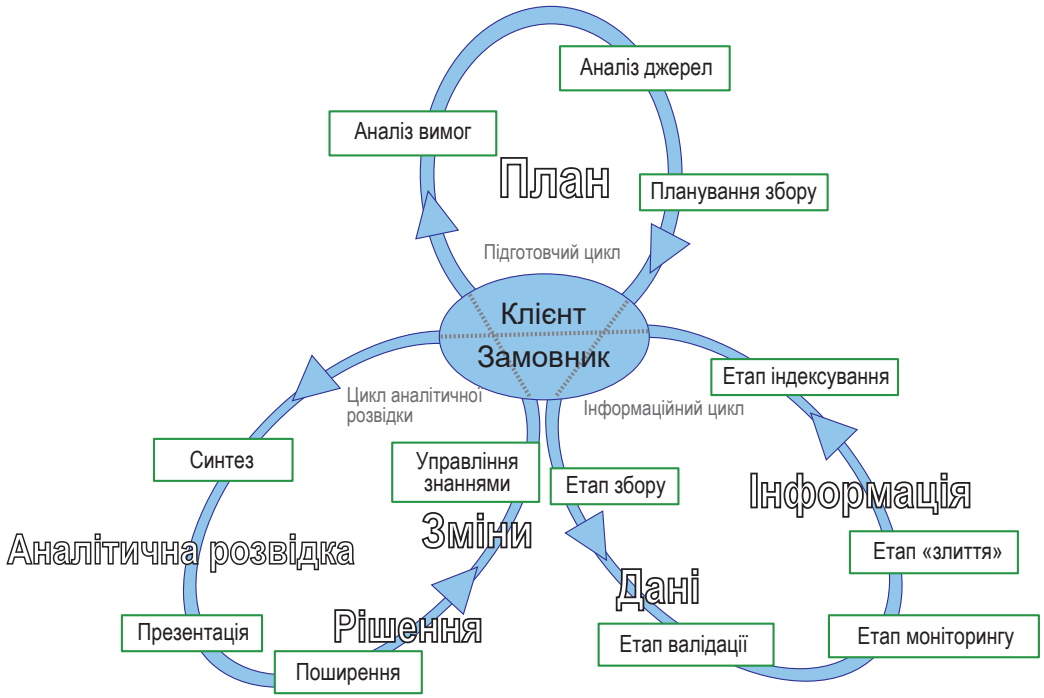


Рисунок 23.1. Цикл OSINT (RIS) [1; 2]

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].

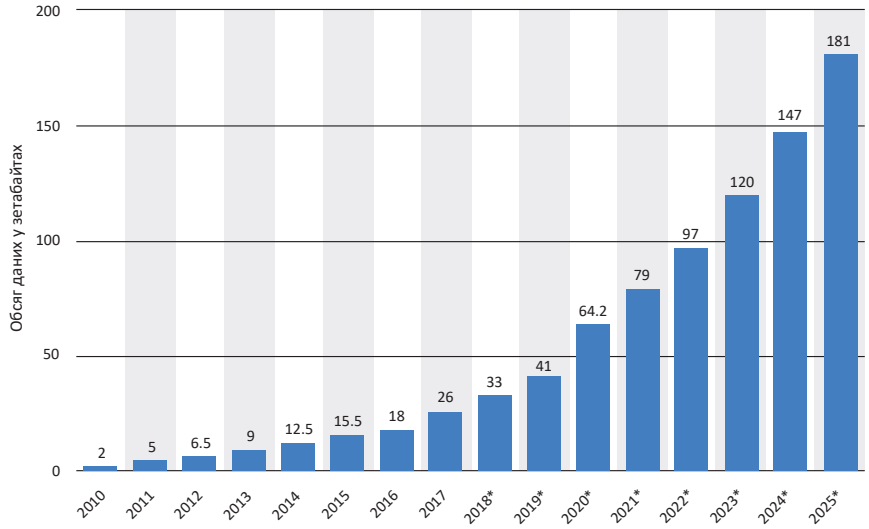


Рисунок 23.2. Загальний обсяг створених, спожитих та збережених даних у всьому світі (2010-2020 роки) та прогноз до 2025 року (Statista, 2023) [1; 5]

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.

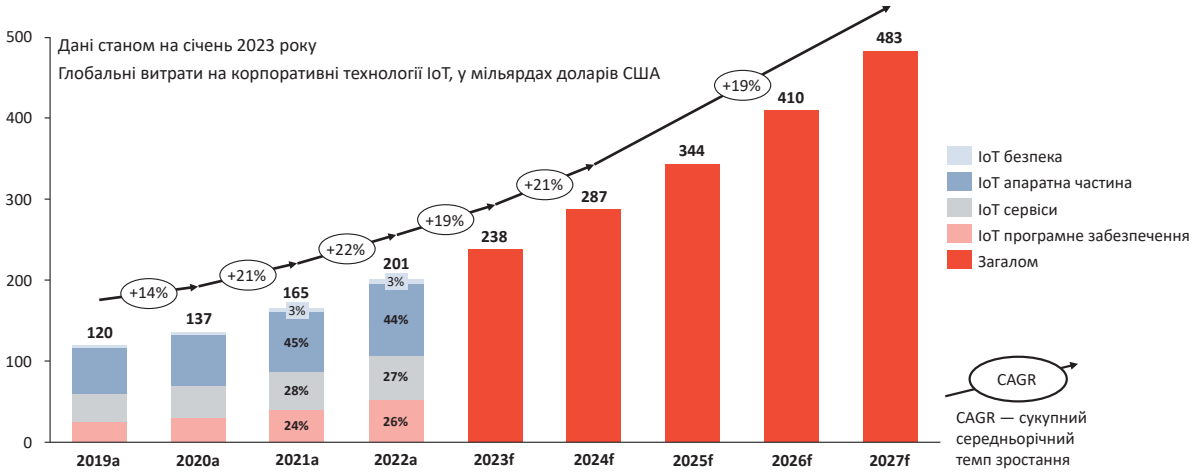


Рисунок 23.3. Аналіз корпоративного ринку IoT (2019-2022 роки) з прогнозуванням до 2027 року (IOT Analytics) [13]

> *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.

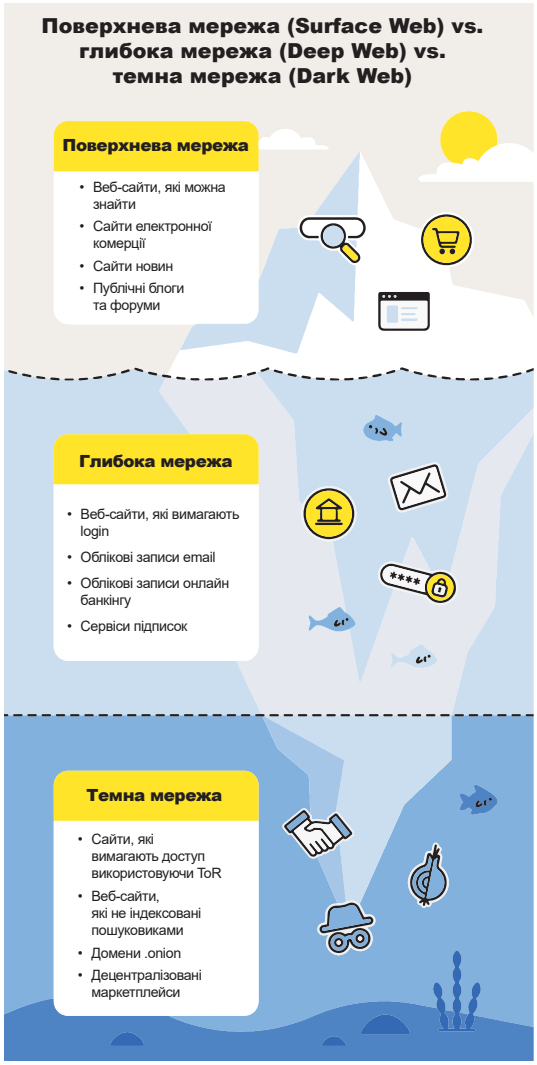


Рисунок 23.4. Мережева структура інтернет: поверхнева, глибока та темні мережі (Norton) [16]

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

DOI: https://doi.org/10.36486/978-966-2310-66-5-24

Майбутні події вже відкидають перед собою тіні
А. Кемпбелл

РОЗДІЛ 24
Тенденції злочинності та прогнозування кримінальної активності

Олена Тихонова
Лариса Герасименко

Ще у 1911 році керівник поліції м. Берклі, штат Каліфорнія Август Воллмер наголосив, що:

> *«Використовуючи припущення регулярності вчинення злочинів та їх подібності, можливо помітити тенденції в певних районах міста, тим самим визначивши місця, пов'язані з високою та низькою ймовірністю вчинення там таких злочинів» [1, с. 1-9].*

Дослідження тенденцій злочинності з використанням можливостей кримінального аналізу є найбільш ефективним при обробці інформації про кримінальні правопорушення серед яких існує висока вірогідність повторності.

> *У випадку вчинення одиночних кримінальних правопорушень застосовувати можливості кримінального аналізу недоцільно [2].*

Вивчення тенденцій злочинності та прогнозування кримінальної активності створює передумови для ефективного запобігання правопорушенням з врахуванням їх специфіки та особливостей. Вивчення тенденцій злочинності дозволяє встановити найбільш актуальні проблеми у сфері боротьби зі злочинністю на певний період часу, визначити пріоритети та оперативні потреби запобігання й протидії їй.

При аналізі тенденцій злочинності використовують кількісні та якісні методи. *Кількісні методи* ґрунтуються на підрахунках і статистичних даних для визначення частоти і значущості злочинної діяльності, обсягу і щільності злочинності, кореляції між злочинністю та іншими факторами, а також майбутніх тенденцій злочинності та оперативних потреб. *Якісні методи* ґрунтуються на безпосередніх спостереженнях суб'єктів, а також на оцінці оперативних даних або іншої інформації. При його проведенні аналізу підлягають матеріали кримінальних проваджень, оперативна інформація, інформація з відкритих джерел, інформація з реєстрів, баз та банків даних, тощо.

> *Для з'ясування тенденцій кримінальної активності доцільно аналізувати її основні кількісно-якісні показники – рівень, динаміка та структура.*

При аналізі тенденцій кримінальної активності розраховують *коефіцієнт інтенсивності злочинності та коефіцієнт злочинної активності*. Перший – відносний показник поширення злочинності на певній території, що визначається через кількість злочинів, яка припадає на кожну тисячу (10 тис., 100 тис.) населення певної території.

$$K = \frac{З \times Нр}{Н},$$

де *З* – кількість злочинів, учинених на території за певний час (абсолютний показник);

$Н_р$ – кількість населення, з урахуванням якої визначається показник інтенсивності злочинності (1 тис., 10 тис., 100 тис.);

Н – чисельність населення на території вираховування в період розрахунку (абсолютний показник).

Зазначений показник дає змогу виявити поширеність певної ознаки в сукупності, що досліджують. Тобто

> *за допомогою **коефіцієнта інтенсивності злочинності** можна виявити те, наскільки уражена злочинністю загалом або окремим її видом певна територія з визначеною кількістю населення, яке проживає на ній.*

Водночас вести мову про зміну інтенсивності злочинності дає підстави не лише зазначений коефіцієнт, а й відповідні зміни у структурі злочинності, що вимірюються в питомій вазі діянь різного ступеня тяжкості. Структурні зміни можуть безпосередньо або опосередковано вказувати на збільшення або зменшення інтенсивності злочинності [3].

Для обрахування поширення злочинності в громаді використовується

> ***коефіцієнт злочинної активності**, який виражає ступінь ураженості різних верств населення злочинністю або певними її видами, а також ступінь поширення різних видів злочинів в окремо визначеному сегменті суспільства.*

Цей показник є певною модифікацією попереднього з єдиною відмінністю – співвідносяться кількість осіб, які вчинили злочини, до усього населення певної території, з розрахунку на яку визначається зазначений показник [4].

$$K = \frac{\text{Озх Нр}}{\text{Н}},$$

де $O_з$ – кількість осіб, які вчинили злочини (абсолютний показник);

$H_р$ – кількість населення, з розрахунку на яку визначається показник злочинної активності (1 тис., 10 тис., 100 тис.);

H – чисельність населення на території вираховування в період розрахунку (абсолютний показник).

Показник, який також дає змогу проаналізувати негативні тенденції поширення злочинності серед певних верств населення, є

> ***коефіцієнт ураженості злочинністю** – це співвідношення питомої ваги злочинців певної категорії, яку вони становлять у загальній кількості злочинців, до всього населення цієї категорії в загальній структурі населення.*

Показник, який так само характеризує тенденції кримінальної активності, є її динаміка, що виявляє зміну рівня (кількісний показник) та структури (якісний показник) злочинності протягом певного часу, тобто цей показник може бути або у відносних, або в абсолютних величинах, а також відображає зміни в часі будь-якої характеристики злочинності. Відображення динаміки рівня злочинності в абсолютних показниках здійснюється за допомогою статистичного часового ряду за відповідними роками. Але найбільш наочним є подання наявного цифрового матеріалу не в таблицях, що ускладнюють загальне сприйняття матеріалу, а у графічному вигляді [5].

Подання цифрового матеріалу за кілька років в абсолютних показниках, як правило, є доволі громіздким для сприйняття і незручним для порівняння. Тому для аналізу такої динаміки злочинності використовують відносні показники, одним з яких є

> ***темп зростання (зменшення) злочинності** – у скільки разів більше (менше) або скільки відсотків становить значення обсягу (рівня) злочинності від аналогічного попереднього (за умови ланцюгового визначення) або базового (за умови базисного визначення) періоду.*

$$\text{T}_\text{p} = \frac{U}{U_{-1}} \text{x} 100\%,$$

де U_i – контрольне значення;

U_{i-1} – попереднє значення того самого показника (або значення базового періоду).

Розрахунок динаміки можливий як для злочинності загалом, так і для окремих проявів злочинної активності. Так само інформативним для характеристики тенденцій злочинної активності є

> *динаміка структурних змін злочинної активності, тобто показників, які відображають кількість або питому вагу злочинної активності (злочинців) певних груп (видів) у їх загальній кількості.*

Ще одним показником, який характеризує тенденції злочинності, є її структура, яка розкриває співвідношення груп або видів кримінальних правопорушень у загальній сукупності злочинності або співвідношення різних категорій осіб, які вчинили кримінальні правопорушення, у загальній структурі виявлених правопорушників або всіх осіб, які фактично вчинили кримінальні правопорушення. Цей показник може бути розрахований як в абсолютних, так і у відносних величинах [6]. *Структура кримінальної активності* може бути визначена за різними ознаками, зокрема:

- *за основними видами кримінальних правопорушень,*

- *основними сферами діяльності, у яких вони вчинюються,*
- *за характерними ознаками осіб, яких було притягнуто до відповідальності,*
- *за розміром установлених та відшкодованих збитків.*

Структура злочинності містить наступну інформацію:

- *питома вага різних видів кримінальних правопорушень за видами;*
- *питома вага розкритих та нерозкритих кримінальних правопорушень;*
- *частки чоловіків, жінок, неповнолітніх, раніше судимих, безробітних, осіб, які вчинили кримінальні правопорушення у стані алкогольного чи наркотичного сп'яніння та інших категорій громадян;*
- *розподіл кримінальних правопорушень за віком суб'єкта (14–15, 16–17, 18–24, 30–49 років, 50 років та старше);*
- *частки ситуативної, рецидивної, професійної, групової, організованої чи озброєної злочинності;*
- *розподіл кримінальних правопорушень за типами населених пунктів (містами і селами), економічно-промисловими районами, за типом місцевості (рівнини, гори, ліси);*
- *розподіл кримінальних правопорушень по порах року;*
- *питома вага осіб, звільнених від кримінальної відповідальності, засуджених до позбавлення волі та інших видів покарання.*

Структура злочинності може бути розрахована також за багатьма іншими кримінально-правовими, кримінологічними, процесуальними, соціально-демографічними та іншими ознаками [7, с. 99].

При аналізі тенденцій злочинності важливо враховувати, що майже всім кримінальним правопорушенням притаманні типові ознаки, що підлягають аналізу. Вони відрізняються залежно від виду протиправного діяння. Типові ознаки важливі тим, що з моменту їх ідентифікації та реєстрації, вони стають доступними для аналізу. Приклад переліку зазначених ознак для аналізу наведено в табл. 24.1 [8].

Таблиця 24.1. Типові ознаки аналізу тенденцій злочинності

Класифікація кримінального правопорушення	Крадіжка, поєднана з проникненням у житло, інше приміщення чи сховище (вид нерухомості: комерційна, житловий об'єкт тощо) Пограбування (поєднаний з насильством, поєднаний з проникненням у житло тощо) Незаконне заволодіння транспортним засобом (приватного автомобіля, комерційного транспорту, мотоциклу тощо) Шахрайство (з використанням підроблених документів, з використанням кредитних карток тощо) Зґвалтування та інші кримінальні правопорушення проти статевої свободи та статевої недоторканості особи (зґвалтування, сексуальне насильство, примушування до вступу у статевий зв'язок тощо) Розбій та вбивство при обтяжуючих обставинах
Географія	Правопорушення за локацією Вулиця, перехрестя, квартал, територія обслуговування, дільниця або район
Хронологія	Кримінальне правопорушення вчинено в певний час Проміжок часу, протягом якого сталося правопорушення (день/ніч) День тижня / Тиждень року / Місяць року
Характеристика потерпілого	Особа потерпілого (стать, вік, національність тощо) Характерні ознаки потерпілого Зв'язок потерпілого з підозрюваним
Особа підозрюваного	Ім'я, вік, національність Зріст, вага, одяг Особливі прикмети
Опис транспортного засобу підозрюваного	Вид транспортного засобу Марка, модель і рік випуску, колір транспортного засобу Наявність пошкоджень транспортного засобу
Опис матеріальних збитків	Вид втраченого майна Ідентифікаційний номер втраченого майна Модель, призначення та використання майна

Окрім вищезазначених типових ознак, існує низка ознак, які є специфічними для конкретного виду злочинів. Ці специфічні ознаки, як правило, відображаються при реєстрації відомостей про вчинення кримінального правопорушення, тому можуть бути використані при проведенні аналізу.

При аналізі тенденцій окремих кримінальних правопорушень важливо ідентифікувати ознаки, притаманні досліджуваному виду правопорушень [8].

Квартирні крадіжки

Типовість квартирної крадіжки визначається моделлю вчинення злочину (*modus operandi*), знання про яку формуються на основі даних про вчинені кримінальні правопорушення. Аналіз квартирних крадіжок ускладнюється на фоні великої кількості зареєстрованих випадків і неспроможністю встановлення чітко виражених характеристик Modus operandi. Одиничний випадок квартирної крадіжки не дасть багато інформації про злочинця. Однак ідентифікована модель крадіжок зі зломом може надати набагато більше інформації, якщо окремі специфічні ознаки ідентифікувати та зіставити між собою.

При аналізі тенденцій квартирних крадіжок важливим є системне вивчення наступних ознак, які розташовані за ступенем значущості для інформативності результатів аналізу:

- ✓ *класифікація кримінального правопорушення;*
- ✓ *географія;*
- ✓ *опис викраденого майна;*
- ✓ *специфічні ознаки Modus operandi;*
- ✓ *опис потерпілого;*
- ✓ *ознаки речових доказів;*
- ✓ *час;*
- ✓ *опис підозрюваного;*
- ✓ *опис транспортного засобу підозрюваного.*

Крадіжки з бізнес-приміщень

Аналіз крадіжок з бізнес-приміщень або крадіжок зі зломом у багатьох відношеннях легший, ніж квартирних крадіжок. Зазначені крадіжки є більш спеціалізованими та демонструватимуть більш специфічні характеристики Modus operandi.

Аналітик має більш конкретну інформацію щодо точки та методу проникнення, опису мети, особи потерпілого та особливостей предмету кримінального правопорушення.

Ознаки часу для крадіжок з бізнес-приміщень можуть бути менш інформативними ніж для аналізу квартирних крадіжок, оскільки більшість досліджуваних крадіжок відбуваються вночі або у вихідні дні.

Особа, яка вчиняє крадіжки з бізнес-приміщень, як правило, більш мобільна порівняно з квартирним крадієм. Зазначений вид кримінального правопорушення має більшу територіальну розгалуженість, адже крадій може подолати значну відстань, щоб потрапити у приміщення, що належить певному бізнесу.

Аналіз крадіжок з бізнес-приміщень має бути системно спрямований на вивчення наступного переліку ознак:

- ✓ *класифікація кримінального правопорушення;*
- ✓ *опис потерпілого;*
- ✓ *специфічні ознаки Modus operandi;*
- ✓ *географія;*
- ✓ *опис викраденого майна;*
- ✓ *ознаки речових доказів;*
- ✓ *опис підозрюваного;*
- ✓ *опис транспортного засобу підозрюваного; час.*

Пограбування

Modus operandi щодо пограбування визначається на основі минулих злочинів як і у випадку з крадіжками. Водночас, оскільки під час пограбування ризик затримання значно вищий, грабіжники частіше схильні змінювати свої схеми поведінки, ніж крадії. При аналізі пограбувань висока ймовірність встановлення потенційної мети злочину. У багатьох випадках грабіжник нападає лише на певну категорію людей або представників бізнес середовища.

При встановленні тенденцій кримінальної активності, кваліфікованої як пограбування особливій увазі підлягає опис підозрюваного, опис викраденого майна та часові особливості. При аналізі квартирних крадіжок першочергове значення мають географічні чинники, тоді як при крадіжках з бізнес-об'єктів значущою є характеристика потерпілого.

При аналізі пограбування важливим є встановлення опису підозрюваного, транспортного засобу та потерпілого, а менш інформативним, з точки зору виявлення тенденцій злочинності, є опис викраденого майна та речових доказів. Також інформативними виявляються відомості про Modus operandi, з метою пов'язування схожих зареєстрованих злочинів.

Аналіз пограбувань має бути системно спрямований на вивчення наступного переліку ознак:
- ✓ *класифікація кримінального правопорушення;*
- ✓ *опис підозрюваного;*
- ✓ *опис потерпілого;*
- ✓ *специфічні ознаки Modus operandi;*
- ✓ *географія;*
- ✓ *опис транспортного засобу підозрюваного;*
- ✓ *час;*
- ✓ *опис викраденого майна;*
- ✓ *ознаки речових доказів.*

Аналіз пограбувань не повинен обмежуватися чітко визначеними географічними районами. Натомість він має охоплювати якомога більшу географію.

Крадіжка транспортних засобів

Особливе значення при встановленні тенденцій даного виду кримінальної активності мають географічні фактори, опис підозрюваного, опис транспортного засобу підозрюваного та опис транспортного засобу, який було викрадено. Перелік ознак, що підлягають аналізу, мають сприйматися з однаковою значущістю:
- ✓ *класифікація кримінального правопорушення;*
- ✓ *географія;*
- ✓ *опис потерпілого;*
- ✓ *час;*
- ✓ *опис транспортного засобу підозрюваного;*
- ✓ *опис викраденого транспортного засобу;*
- ✓ *речові докази.*

При вивченні конкретних особливостей Modus operandi при викраденні транспортного засобу увага акцентується на стані транспортного засобу під час виявлення. Першочерговими факторами при аналізі випадків викрадення транспортного засобу є місце повернення, марка та модель, а також ступінь пошкодження викраденого транспортного засобу.

Зґвалтування та інші злочини сексуального характеру

Поглиблений аналіз зґвалтувань і сексуальних злочинів має бути акцентований на тих випадках, у яких немає очевидного зв'язку між особою підозрюваного і особою потерпілого. Коли особа ґвалтівника або сексуального злочинця вчиняє злочини типу «від незнайомця до незнайомця» можна встановити типові особливості Modus operandi. Аналіз зґвалтувань та інших злочинів сексуального характеру має бути системно спрямований на вивчення наступного переліку ознак:
- ✓ *класифікація кримінального правопорушення;*
- ✓ *географія;*
- ✓ *опис потерпілого;*
- ✓ *час;*
- ✓ *опис підозрілих транспортних засобів;*
- ✓ *відносини підозрюваного-жертви; речові докази.*

ПАТЕРНИ

При аналізі тенденцій кримінальної активності важливу роль відіграє визначення патернів. Їх особливе значення обґрунтовується тим, що вони є «ядром» так званого закону аналітики:

> *«Найбільш чітким індикатором потенційної злочинної діяльності є аналогічні дії, що вчиняються зараз» [9, с. 34].*

Злочинці, які сформували свої наміри та «успішно» їх реалізували, скориставшись певною можливістю, будуть мотивовані на продовження кримінальної активності, що формує базові знання для встановлення моделі кримінальної діяльності, ознак повторюваної активності тобто патернів.

> *Менеджмент патернів (обставин інцидентів та поведінкової специфіки) буде оптимальним форматом на відміну від індивідуальних розслідувань [10, с. 37].*

Навіть дескриптивний аналіз патернів, вчинених у минулому кримінальних правопорушень, може бути використаний для прогнозування майбутньої динаміки. Ідентифікація патернів є передумовою ефективного запобігання злочинності, адже незважаючи на можливість виникнення певних відхилень у короткостроковій перспективі, більшість тенденцій та проблем залишаються незмінними до моменту прийняття рішення про вжиття дієвих заходів [11].

> *Аналіз патернів щодо вчинених у минулому злочинів може бути використаний для прогнозування майбутньої динаміки [12].*

Основою для встановлення патерну може слугувати час (дата і день тижня, а також кількість днів між зафіксованими інцидентами), географічне розташування (локації (міські, приміські або сільські), види діяльності, характерні для визначеного місця (комерційні, промислові, житлові райони), висотність, наближеність до інших житлових (або нежитлових) будівель тощо.

Під час вивчення тенденцій кримінальної активності можуть бути виявлені наступні патерни:

«Серія» - два чи більше подібних кримінальних правопорушення, вчинених тією самою особою чи групою осіб, які діють за попередньою змовою

> ***наприклад**, грабіжник «зазирає» у шість аптек за три місяці й завжди викрадає наркотичні знеболюючі речовини; гвалтівник вишукає жертв-жінок, представляючись брокером зі здачі нерухомості в оренду та заманюючи їх у порожні квартири; одна банда здійснює напади на дванадцять компаній, приміщення яких розташовані в діловому центрі;*

«Хвиля» - серії кримінальних правопорушень, інтервал між якими настільки короткий, що вони видаються безперервними

> ***наприклад**, викрадення транспортних засобів, що було вчинено протягом липня в одному районі міста та викрадення транспортних засобів, що було вчинено протягом серпня в іншому районі того самого міста;*

«Гаряча здобич» («Hot Prey») - патерн, що характеризується однотипністю постраждалих

> ***наприклад**, із наближенням місцевих виборів на посаду мера громадяни, які підтримують одного кандидата, починають масово повідомляти про акти вандалізму, вчинені щодо їхніх домівок та авто;*

«Гарячий об'єкт» («Hot Product») - патерн, що характеризується однотипністю вкраденого майна

> ***наприклад**, відкривається новий ломбард, який скуповує мобільні телефони, і за які розраховується готівкою – рівень крадіжок мобільних телефонів різко зростає;*

«Гаряче місце» («Hot Place») - патерн, у рамках якого всі інциденти відбуваються в одному й тому самому місці

> ***наприклад**, кінотеатр подовжує у вечірній час термін показу кінофільмів. Упродовж чотирьох місяців з моменту такого оголошення особами, які «тусуються» на паркувальному майданчику для автомобілів, було вчинено 8 пограбувань;*

«Гаряче середовище» («Hot Setting») - патерн, що характеризується однотипністю місця інциденту

> ***наприклад**, крадіжка мідних труб з будівельних майданчиків у всьому місті;*

«Рецидивні злочини» («Hot Incidents») - певні місця, люди, види діяльності настільки ідентичні, що одну справу важко відрізнити від іншої.

Алгоритм аналізу патернів

Під час аналізу патернів необхідно отримати відповіді на низку питань, зокрема:

- ✓ ***Що?***
  - *тип та характеристики злочину*
  - *послідовність подій*
  - *діяння осіб, що брали участь у події*
- ✓ ***Де?***
  - *конкретне місце*
  - *тип місцевості*
  - *середовище*
  - *маршрут підходу та відходу (місце першого контакту, місце вчинення кримінального правопорушення, місце виявлення)*
  - *напрям пересування*
  - *географічне прогресування патерну*
  - *територіальна близькість інших пов'язаних або споріднених подій*
- ✓ ***Коли?***
  - *час доби*
  - *день тижня*
  - *тиждень місяця*

- *місяць року*
- *сезон*
- *кількість днів між подіями*

✓ ***Хто?***
- *правопорушник (характеристика особи правопорушника; автомобіль; діяльність до та після правопорушення; мотив)*
- *потерпілий (характеристика особи потерпілого; діяльність до та після)*

✓ ***Як?*** *(Modus operandi - спосіб вчинення кримінального правопорушення)*
- *знаряддя*
- *нанесені ушкодження*
- *шкода, заподіяна майну*
- *«почерк» (як правопорушник вчиняє кримінальне правопорушення; що незвичного в тому, яким способом правопорушник вчиняє кримінальне правопорушення; що унікального в тому, яким способом правопорушник вчиняє кримінальне правопорушення)*

✓ ***Чому?***
- *чому саме це кримінальне правопорушення?*
- *чому саме ця ціль?*
- *чому саме цей час?*
- *чому саме це місце?*
- *чому саме цей спосіб вчинення кримінального правопорушення?*

ПРОГНОЗУВАННЯ КРИМІНАЛЬНОЇ АКТИВНОСТІ

Встановлення тенденцій злочинної активності дозволяє спрогнозувати її розвиток. При цьому варто враховувати, що в сфері людської діяльності, до якої відноситься й кримінальна активність, виходячи виключно з даних, невідомим залишається будь-який цикл, не дивлячись на його повторюваність з регулярністю, на основі якої можна було б скласти певний прогноз на майбутнє. Разом з тим відомості про який-небудь цикл, взяті в сукупності з іншими даними, корисні.

> ***Прогнозування*** *- це дослідження, що базується на всебічному аналізі ретроспективного розвитку та глибокому знанні об'єктивних законів і має на меті наукове обґрунтування розвитку кримінальної активності у майбутньому, а також визначення альтернативних шляхів, строків та умов її розвитку.*

Воно не зводиться до спроб однозначного передбачення виникнення тих чи інших змін. Прогнозування – багатоступеневий процес, який передбачає постановку цілей, отримання інформації, її обробку, оцінку і аналіз, визначення перспектив і ймовірності реалізації прогнозу.

> ***Основне завдання прогнозування*** *– виявити закономірні тенденції, дослідити та врахувати фактори, що визначають найбільш ймовірний варіант розвитку кримінальної активності [13].*

Прогноз – процес аргументованого передбачення на підставі глибокого аналізу і узагальнення наявних даних майбутнього стану певного виду кримінальної активності та її характеристик, а також напряму, характеру та особливостей розвитку явищ та процесів деструктивного характеру, які спостерігаються. Він спрямований тільки на майбутнє. Прогнози є свого роду «передбаченням» майбутньої подій на основі аналізу минулих і сучасних тенденцій.

> *Прогнозування можна здійснювати як з використанням статистичних, так і описових даних.*

Кожен прогноз розробляється так, щоб уникнути небажаних результатів можливого перебігу кримінальної активності і прискорення ймовірного їх розвитку в потрібному напрямі.

Прогнози виявляють ймовірнісну картину очікуваних подій, вони багатоваріантні і мають рекомендований характер. Наукове прогнозування вказує напрям розвитку певних закономірних тенденцій, визначає терміни їх повного прояву. Усі прогнози, незалежно від строків упередження і сили передбачення, спрямовані або на передбачення наслідків розвитку існуючих тенденцій та з'ясування можливості їх перетворення, або на передбачення появи нових тенденцій.

Основні функції прогнозування кримінальної активності:
- *науковий аналіз процесів і тенденцій;*
- *дослідження об'єктивних зв'язків;*
- *визначення факторів та рівнів їх впливу;*
- *оцінка об'єкта прогнозування;*
- *виявлення альтернатив розвитку процесів та явищ;*

- *накопичення матеріалу для планування, проектування та вибору управлінських рішень.*

Для того щоб прогноз був достовірним та максимально наближеним до фактичного розвитку подій, необхідно:
- *точно й однозначно сформулювати проблему (мету, завдання);*
- *визначити предмет та об'єкт;*
- *зібрати повну (за структурою, обсягом, змістом) та достовірну інформацію про об'єкт, привести її у зіставний вигляд;*
- *провести повноцінний системний аналіз вихідної інформації;*
- *чітко структурувати основні й побічні ефекти;*
- *ранжувати параметри впливу за значущістю;*
- *чітко визначити прогнозний період (інтервал або проміжок часу, протягом якого необхідно передбачити процеси, що відбуваються з об'єктом);*
- *визначити методологію проведення прогнозу — від збору та обробки даних до розрахунку кінцевих параметрів;*
- *визначити процедуру перевірки правильності отриманих у результаті прогнозу результатів.*

До методів прогнозування належать:
- *фактографічні методи;*
- *експертні методи;*
- *методи екстраполяційного прогнозування;*
- *методи цільового прогнозування;*
- *метод передбачення Локвуда;*
- *метод аналізу конкуруючих гіпотез Р.Хейера.*

Правила складання прогнозу кримінальної активності:
- *необхідно обрати тип прогнозу залежно від поставленого завдання;*
- *врахувати якнайбільше чинників, керуючись принципом повноти;*
- *мета прогнозу має відповідати ступеню деталізації чинників і межі розподілу їх на окремі предмети;*
- *необхідно обрати найбільш важливі чинники;*
- *під час складання списку чинників враховувати ступінь інтенсивності їхнього вияву.*

Вибір зазначених чинників відбувається на основі знань відповідно минулого і теперішнього розвитку кримінальної активності, яка підлягає дослідженню.

Розробка прогнозу є сукупністю трьох послідовних процедур:
- ***ретроспективи**, яка полягає у дослідженні типових подій і ситуацій у минулому, а також цілого комплексу явищ, подій і ситуацій (економічних, політичних, воєнних, етносоціальних факторів), які спричинили теперішній стан кримінальної активності;*
- ***діагнозу** - опису, пояснення поточного стану явищ, подій і ситуацій і побудови його базисної теоретичної моделі;*
- ***проекції** - побудови на базі діагнозу можливих варіантів розвитку явищ, подій і ситуацій й розрахунку можливих наслідків.*

Способи побудови проекції:
- *оцінювання перспектив розвитку конкретного явища, події або ситуації на основі аналогії з добре відомими подібними явищами, подіями чи ситуаціями;*
- *перенесення у майбутнє тенденцій розвитку кримінальної активності, яка існували в минулому і має місце нині;*
- *модельне уявлення про майбутнє.*

При розробці методології прогнозування необхідно з'ясувати, який принцип повинен бути покладений в основу прогнозування, з чого потрібно виходити при прогнозуванні, які фактори чинять вирішальний вплив на розвиток кримінальної активності в майбутньому.

В основу прогнозування може бути покладений один з наступних принципів.

Прогнозування на основі врахування стійких тенденцій

У цьому випадку потрібно виходити з припущення, що при відсутності даних, що вказують на протилежне, дане положення не зазнає значних змін протягом періоду, що охоплюється прогнозом.

Складаючи прогноз, в переважній кількості випадків потрібно враховувати такий фактор, як стійкість положення. Будь-який прогноз будь-якого явища враховує стійкі тенденції, виходить з незмінності положення навіть в тих складних випадках, коли прогноз стосується нестійкого явища, яким і є кримінальна активність. Аналітичні прогнози, як правило, стосуються визначеного кола кримінальної активності.

Прогнозування на основі врахування розвитку подій

Цей принцип застосовується в тих випадках, коли існує якась певна тенденція розвитку кримінальної активності на висхідній лінії (позитивний тренд). І ми припускаємо, що на період, який охоплюється прогнозуванням, крива розвитку буде йти в тому ж напрямі, що і раніше, якщо відсутні дані, що свідчать про протилежне.

Прогнозування на основі врахування циклічного розвитку подій

Припливи та відпливи характерні не тільки для океанів, але також і для розвитку багатьох інших явищ, у тому числі, кримінальної активності. Кримінальна активність зростає та спадає, причому цикли ці мають нерегулярний характер та формуються як під впливом зовнішнього середовища, так і під впливом внутрішніх факторів. Прогнозування, засноване на врахуванні циклічного розвитку подій, частково виходить з припущення, що історія в певній мірі повторюється, тобто, кримінальна активність, що розвивалася у минулому циклічно, і дальше буде розвиватися таким же чином. Очевидно, якщо певна кримінальна активність розвивається циклічно, то прогнози, які відбувалися, виходячи з припущення, що її розвиток відбувається в одному напрямі протягом тривалого часу, є помилковими.

ВІЗУАЛІЗАЦІЯ ПРОГНОЗІВ

При прогнозуванні кримінальної активності, поряд із збиранням та попередньою обробкою даних, важливою є їх візуалізація.

> *Основна мета візуалізації даних – чітко та ефективно транслювати дані за допомогою статистичних графіків.*

Якісна візуалізація допомагає здійснювати ефективний аналіз та формувати відповідні гіпотези на основі наявних відомостей щодо кримінальної активності. Робота з візуалізації передбачає створення карт щільності злочинності, що допомагають аналітикам аналізувати моделі кримінальної активності. Розуміння таких моделей є важливим елементом досудового розслідування кримінальних правопорушень та розроблення заходів запобігання злочинності.

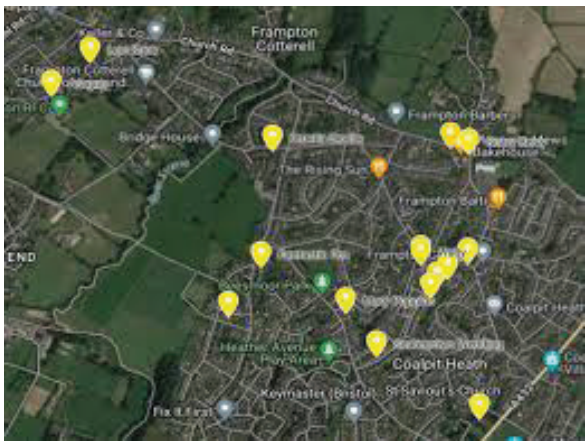


Рисунок 24.1. Місця вчинення кримінальних правопорушень

Аналіз інформації про кримінальну активність, що спостерігається на певній місцевості, є більш інформативним за умови використання карт, на які екстрапольовано відомості щодо досліджуваного явища. Одним з ефективних інструментів для візуалізації відомостей при прогнозуванні кримінальної активності є Google Maps. Цей модуль спираючись на дані про злочини з набору даних, зокрема, щодо географічних координат (довготи та широти), позначає на карті конкретні місця розташування. У ході зазначеного тегування також відображається назва місця злочину та тип злочину, який було вчинено [14].

Ця інформація є корисною для людини, яка знає небезпечні та ризикові зони, і тому може визначити на карті такі території. Зазначена інформація може бути корисна з точки зору запобігання кримінальній активності. На рис. 24.1 продемонстровано кримінальну активність на території певної громади. Виходячи з аналізу скупченості вчинених правопорушень, аналітик може зробити висновок щодо можливості вчинення конкретних злочинів у майбутньому, як на тій самій території, так і на суміжній.

Також за допомогою Google Maps є можливість в інтерактивному форматі візуалізувати територію (рис. 24.2), де було вчинено кримінальне правопорушення. Інтерактивне зображення допомагає правоохоронним органам отримати інформацію щодо запроваджених заходів безпеки на зазначеній території, а також визначити, в якому місці може бути наступна кримінальна активність [15].



Рис. 24.2. Інтерактивне зображення місця вчинення злочину.

Крім того, Google Maps дає можливість візуалізувати на карті різні види злочинів, що було вчинено на певній території (рис. 24.3). Завдяки такій візуалізації аналітик може визначитись

які види кримінальних правопорушень найчастіше вчиняються на території, а також розробити заходи безпеки з врахуванням отриманої інформації.

За допомогою Google Maps можна візуалізувати «hot spots» («гарячі точки») кримінальної активності - територія на карті, де спостерігається висока щільність таких проявів (рис. 24.4). «Hot spots» використовуються аналітиками для вивчення появи гарячих точок у певних регіонах, а також причин та умов, які сприяють цьому [16].

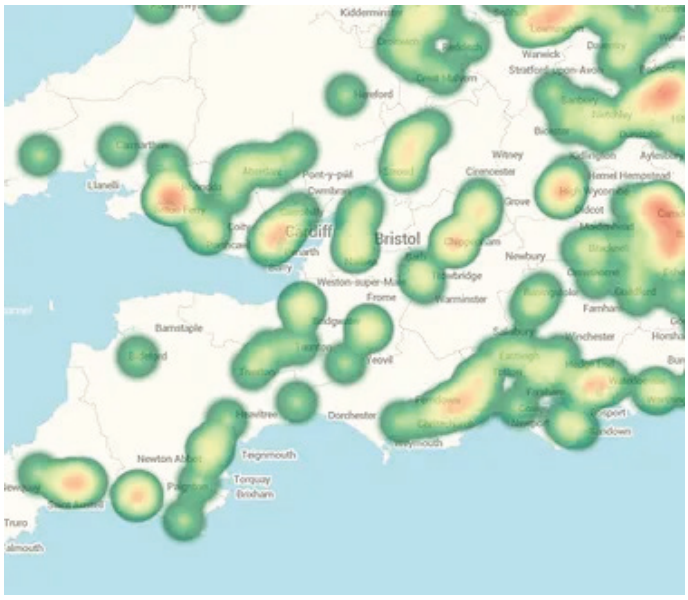


Рисунок 24.4. Візуалізація «hot spots»

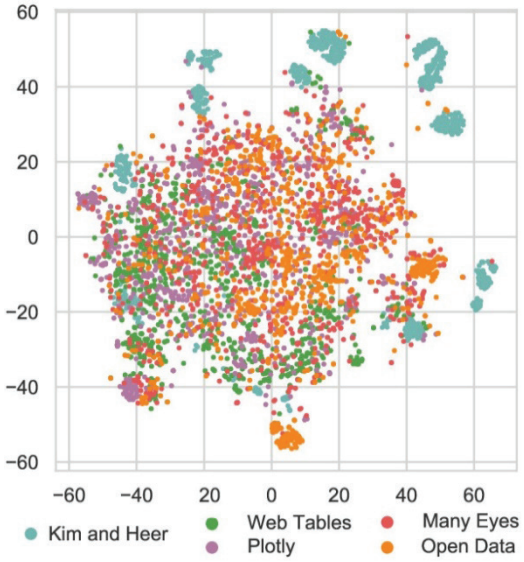


Рисунок 24.3. Типи кримінальних правопорушень, що було вчинено на території

Завдяки зазначеній інформації можливо проаналізувати кримінальну активність на певній місцевості. Результати такого аналізу можуть бути використані для прийняття найбільш оптимальних рішень щодо розподілу сил та засобів та формування стратегії протидії злочинності.

Під час прогнозування важливо враховувати наступні моменти:

- *Чи є очікувана тенденція новою або добре знайомою?*
- *Якщо спостерігаються будь-які зміни щодо способу дії, особи лідера, стратегії та інших важливих аспектів діяльності злочинної групи необхідно визначити ступінь значущості таких змін.*
- *Розділяйте середньострокові та довгострокові зміни*
- *З'ясуйте причину виникнення змін.*
- *Які обмежуючі фактори можуть впливати на зміни?*
- *Ідентифікуйте суттєві обставини чи зазначте, якщо це доцільно, свої сумніви.*
- *Вкажіть на «сірі зони» (питання, відповіді на які не є однозначними).*
- *Вкажіть припущення, які вплинули на формування прогнозів.*

Таким чином, встановлення тенденцій та прогнозування злочинної активності, а також якісна візуалізація отриманої інформації сприяють розробленню ефективних заходів протидії злочинності, враховуючи і профілактику.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Grassie, R.P., Waymire, R.V., Burrows, J.W., Anderson, C.L. R. & Wallace, W.D. (1977). *Crime analysis executive manual.* Washington, DC: U.S. Department of Justice, Law Enforcement Assistance Administration.
2. Тихонова О.В. Кримінальний аналіз як дієвий засіб викриття корупційних схем. *Корупційна злочинність у міжнародному вимірі: форми, методи та засоби протидії*: матеріали Міжнародного круглого столу (Київ, 9-10 листопада 2017 р.). Київ, 2017. С. 64–66.
3. Тихонова О.В. Фінансова безпеки України: кримінально-правові та кримінологічні основи: монографія. Дніпропетровськ, 2015. 484 с.
4. Носач А. Кримінологічний аналіз кількісних та якісних показників злочинів проти державного суверенітету і територіальної цілісності України. *National Law Journal: Theory and Practice.* 2019. August. С. 146-151.
5. Джужа О.М., Василевич В.В., Кулик О.Г. Основні показники злочинності: міжнародний і вітчизняний досвід. *Вісник Верховного Суду України.* 2012. № 1 (137). С. 37-42.
6. Бабенко А.М. Регіональна злочинність в Україні: закономірності, детермінація та запобігання: дис. … д-ра юрид. наук: 12.00.08. Запоріжжя, 2015. 515 с.

7. Кримінальний аналіз та аналіз ризиків. Загальне керівництво для правоохоронних органів Республіки Молдова та України. 2017. 130 с.
8. Austin, R., Cooper, G., Gagnon, D., Hodges, J., Martensen, K. & O'Neal M. *Police crime analysis unit handbook*. Washington, 1973.
9. Користін О.Є., Пефтієв Д.О., Пеньков С.В., Некрасов В.А. Довідник керівника поліції - поліцейська діяльність, керована розвідувальною аналітикою / ILP. Київ: «Видавництво Людмила», 2019. 120 с.
10. Користін О.Є. Розвиток стратегічної безпекової компоненти на основі «Intelligence». *Вивчення криміногенної ситуації в Україні та прогнозування її подальшої динаміки (вплив воєнних факторів)*: матеріали науково-практичного круглого столу (м. Київ, 07 верес. 2022 р.). Київ: ДНДІ МВС України; Харків: Мачулін. 2022. С. 34-38.
11. Цимбалюк М.М., Шандра Б.Б. Філософсько-правова характеристика злочинності : соціокультурні реалії: монографія. Львів: Ліга-прес, 2016. 254 с.
12. Користін О.Є. Безпекова модель на основі «Intelligence». *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України:* матеріали міжвідомчої науково-практичної конференції (м. Київ, 11 серп. 2022 р.). Київ, 2022. С. 86-90.
13. Рог В.Є., Мелащенко О.П. Статистичний аналіз: виявлення факторів, які обумовлюють стан та динаміку злочинності. *Теоретичні питання юриспруденції і проблеми правозастосування: виклики XXI століття*: тези доповідей учасників III Всеукраїнської науково-практично конференції (м. Харків, 19 черв. 2020 р.). Харків, 2020. С. 192-194.
14. Hitesh Kumar Reddy ToppiReddy et al. (2018). Crime Prediction & Monitoring Framework Based on Spatial Analysis. *Procedia Computer Science, 132, 696–705*.
15. Gesmann, M. & de Castillo, D. (2011). Using the Google visualisation API with R. *The R Journal, 3(2), 40-44*.
16. Crime Petrol. Retrieved from https://en.wikipedia.org/

DOI: https://doi.org/10.36486/978-966-2310-66-5-25

Найнебезпечніші – аж ніяк не ризики, які ви можете побачити і виміряти, а ризики, які ви не можете побачити і, отже, виміряти

Чарльз Віллан

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

Вячеслав Некрасов
Грігол Катамадзе

МЕТОДОЛОГІЧНІ ЗАСАДИ ЗАСТОСУВАННЯ РОП

Процес формування сучасного правоохоронця (детектива (слідчого, оперативного працівника), аналітика) вимагає глибоких знань методології аналізу ризиків та управління ними, складної системи «правоохоронець – кримінальне явище», як сучасного інструментарію управління безпекою, в якій враховуються впливи людського чинника, надійності системи, зовнішніх факторів небезпек на інтегральний рівень безпеки. В основі управління безпекою лежить системний підхід до виявлення джерел небезпеки і контролю чинників ризику на користь зведення до мінімуму людських жертв, матеріального збитку, а також фінансових, екологічних і соціальних втрат.

Ключовим моментом впровадження ризик-орієнтованого підходу (- *далі РОП*) в Україні в питаннях протидії злочинності стало прийняття Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» (п.53 ч.1 ст.1, п.3 ч.1 ст.3, ст.7) [1], а також включення в Закон України «Про Бюро економічної безпеки України» 2021 р. [2] (п.7 ч.1 ст.1, ст.12), положень такого характеру, а видання Указу Президента України «Про запровадження національної системи стійкості» [3], лише посилило актуальність реалізації у правоохоронній практиці такого підходу.

Хоча в широку практику протидії злочинності принципи РОП ще не увійшли, вони одержали визнання в розвинених країнах при вирішенні проблем безпеки в суспільстві.

> *Широке впровадження цієї практики в діяльність усіх правоохоронних органів це прояв здатності держави вирішувати проблеми, що мають системний характер.*

Розглядати злочинність саме як кримінальну загрозу, а діяльність правоохоронних органів та інших суб'єктів контролю через призму спроможності державних інститутів щодо відвернення її проявів, допомагає сформувати принципово інші підходи до системи організації роботи правоохоронного сектору, зокрема в питаннях досудового розслідування, оперативно-розшукової діяльності, аналітичної діяльності та використання штучного інтелекту в правоохоронній практиці. У такому випадку реалізація превентивної функції в діяльності правоохоронних органів, що спрямована на мінімізацію кримінальних ризиків, стає цілком реалістичним проектом.

> *Чому саме РОП є наріжним каменем на якому треба будувати сучасну правоохоронну систему?*

По-перше, ризик є однією з системоутворюючих складових національної, економічної, публічної безпеки, відповідно аналіз ризиків є інструментом вивчення складних соціально-економічних систем в умовах невизначеності. Ризик – це ймовірність виникнення негативного наслідку конкретної діяльності, загроза понесення певних збитків, результат впливу невизначеності на досягнення поставленої мети;

По-друге, складовими ризику є загроза як потенційна, можлива небезпека, що має намір та можливості заподіяти шкоду національній, економічній, публічній безпеці, котрі характеризуються масштабом (впливом) та ймовірністю її реалізації. Тобто йдеться про сили, явища та чинники, а такою є протиправна діяльність оргзлочинності, сама наявність яких вже передбачає застосування до них заходів з боку правоохоронних органів, а також інших суб'єктів контролю ще під час формування наміру та визначення можливостей. При цьому ідентифікація уразливостей (проблеми,

вади, недоліки) систем національної, економічної, публічної безпеки, які породжують або посилюють піддатливість негативним впливам загроз надає можливість визначити шляхи підвищення спроможності системи;

По-третє, в РОП ми завжди маємо справу з ймовірнісними категоріями, розрахунками можливого впливу та працюємо над тим, щоб не допустити реалізацію загрози, мінімізувати її вплив або мінімізувати наслідки;

По-четверте, виходячи з принципу контрінтуїтивної поведінки Дж. Форрестера (1974, 1978), базуючись на принципах роботи складних систем, якими є національна, економічна, публічна безпеки, дати задовільний прогноз поведінки складної системи на досить великому проміжку часу, спираючись тільки на власний досвід та інтуїцію, практично неможливо. Це пов'язане з тим, що наша інтуїція «вихована» на спілкуванні з простими системами, де зв'язки елементів практично завжди вдається простежити. Контрінтуїтивна поведінка складної системи полягає в тому, що вона реагує на вплив зовсім іншим чином, ніж це нами інтуїтивно очікувалося [4]. Тому інструментарій аналізу ризику яким повинні оперувати працівники правоохоронного органу побудовані на обробці великих масивів інформації саме штучним інтелектом (машиною) із застосуванням спеціальних методик та алгоритмів роботи.

По-п'яте, РОП також оперує інструментами, які надають можливість визначити зону компетенцій кожного суб'єкта контролю у забезпеченні національної, економічної, публічної безпеки, розкриваючи її через наявність або відсутність достатніх оперативних можливостей (людських, технічних ресурсів тощо), юридичних повноважень, компетентностей тощо.

Таким чином, метою розроблення методології із застосування РОП є опис системних підходів до оцінки ризиків національної, економічної, публічної безпеки, які базуються на поєднанні об'єктивних кількісних статистичних даних і суб'єктивних якісних експертних оцінок, аналізу агентурно-оперативної інформації правоохоронних органів (співбесіди, опитувальники), результатів розгляду кримінальних проваджень, оперативно-розшукових справ, заходів, які вживаються суб'єктами контролю у сфері забезпечення національної, економічної, публічної безпеки, приватним сектором та інших прикладів міжнародного співробітництва між правоохоронними органами з протидії кримінальним загрозам, а також іншої інформації з відкритих джерел. РОП призначений для структуризації аналізу доступної інформації про загрози, вразливості і можливі наслідки прояву ризиків, пов'язаних із забезпеченням національної, економічної, публічної безпеки, з метою покращення управлінської діяльності, обґрунтованого застосування заходів реагування на ризики та для впровадження основних результатів міжнародних практичних і методологічних досліджень, а також для врахування національних особливостей застосування РОП у правоохоронній практиці.

Враховуючи вищезазначене, запровадження РОП саме у правоохоронній діяльності матиме значний економічний ефект, сприятиме вирішенню системних проблем, здатне постійно утримувати рівень компетентностей в актуальному стані.

Загальні підходи та принципи застосування РОП

> ***РОП*** *– це визначення (виявлення), оцінка (переоцінка) та розуміння ризиків, а також вжиття відповідних заходів щодо управління виявленими ризиками у спосіб та в обсязі, що забезпечують мінімізацію таких ризиків залежно від їх рівня [2].*

Застосування РОП правоохоронними органами, які опікуються питаннями забезпечення національної, економічної, публічної безпеки тощо, здійснюється у порядку, визначеному їх внутрішніми документами, з урахуванням підходів окреслених для центральних органів виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України. Внутрішні документи повинні, містити програму управління ризиками національної, економічної, публічної безпеки, що враховує визначення ризиковості окремих осіб, груп, юридичних осіб та об'єктів, ризики процесів та діяльності, використання існуючих організаційних форм підприємництва у злочинних цілях, включаючи ризик використання технологічних досягнень, ризик-рішення та ризик-послуги розпорядників бюджетних коштів тощо.

Кінцевою метою застосування РОП є виявлення (актуалізація) кримінальних ризиків (загроз, вразливостей, наслідків) в системі забезпечення національної, економічної, публічної безпеки, визначення елементів управління ними та сприяння у розробці стратегії розвитку системи національної, економічної, публічної безпеки.

> ***Ризик*** *- ймовірність виникнення негативного наслідку конкретної діяльності, загроза понесення певних збитків, результат впливу невизначеності на досягнення поставленої мети. Ризик складається з імовірності реалізації загрози та вразливості об'єкта, якому загрожує загроза та результатів впливу.*

Загроза – наявність сили, явищ та чинників, що мають намір та можливості заподіяти шкоду національній, економічній, публічній безпеці, котрі характеризуються масштабом та ймовірністю її реалізації.

Уразливість - наявність проблем, вад, недоліків системи, які породжують або посилюють схильність до порушення функціональності та/або піддатливість негативним впливам загроз національній, економічній, публічній безпеці. При їх оцінці одним із компонентів є негативний вплив, а іншим - механізм контролю.

Вплив - ймовірні (прогнозовані) наслідки реалізації загрози або виникнення інших явищ і чинників, які не становлять загрозу, але можуть вплинути на національну, економічну, публічну безпеки. Це відображає рівень економічної, емоційної, фізичної, інтелектуальної та політичної шкоди, яка може статися у разі реалізації загрози. Рівень впливу залежить від рівня самої загрози, а також від вразливості об'єкта, що перебуває під загрозою, та його здатності відвернути загрозу.

Ймовірність - показник, який характеризує можливість реалізації певних подій, інцидентів, загроз або їх наслідків.

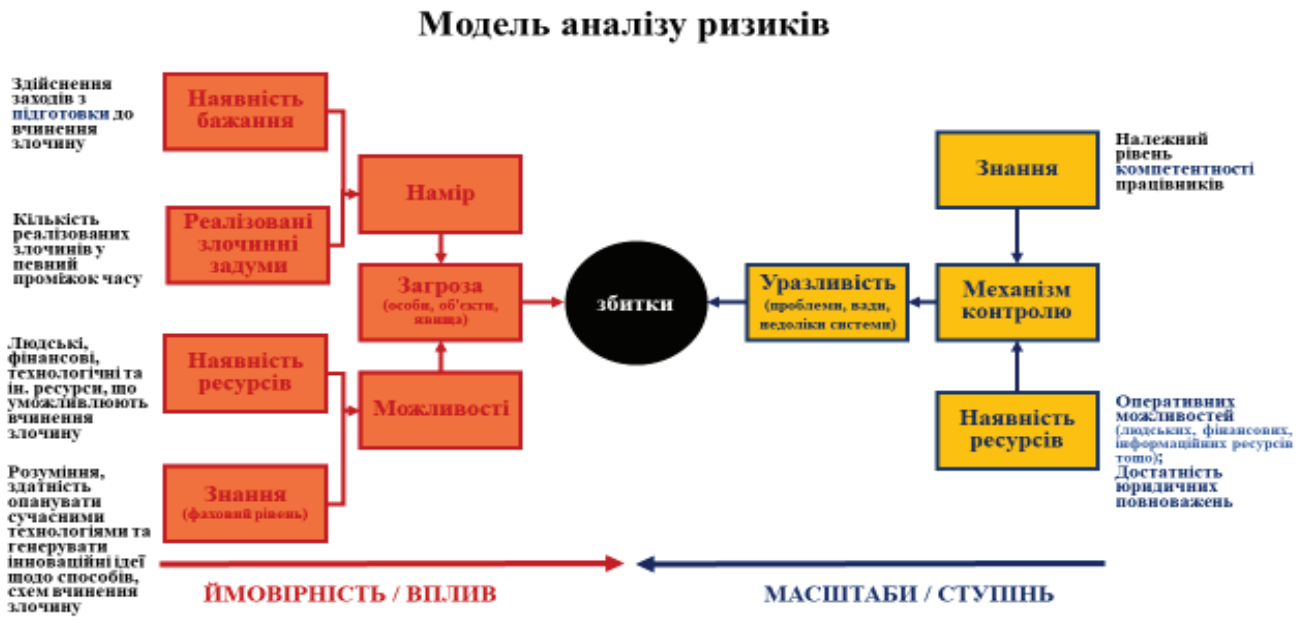
Компетентність - здатність, аналітика, детектива, керівника ефективно застосувати здобуті ними знання, уміння, навички для реагування на кримінальні загрози економічній безпеці на будь-якому етапі.

Механізм контролю – наявні знання та ресурси, що можуть бути використані для реагування на загрозу, підвищення стійкості та зменшення уразливості.

Можливість - це володіння знаннями та ресурсами, необхідними для реалізації наміру.

Намір – задум, бажання щось зробити або здійснити, передбачаючи та приймаючи наслідки.

Фактор ризику - це змінна, що підсилює виникнення, реалізацію та наслідки кримінальної загрози.



РОП спрямований на:

- сприяння виробленню проактивної стратегії і тактики стримування щодо застосування в економіці, суспільстві та в сфері управління публічними фінансами кримінальних бізнес-моделей (схем, способів вчинення злочинів), шляхом впливу на кримінальний попит та кримінальні пропозиції, які домінують в цих сферах (на тіньовому ринку), а також осіб, які генерують такі ідеї, усунення інших факторів, які сприяють криміналізації суспільних відносин;
- запобігання вчиненню кримінальних правопорушень, шляхом руйнування кримінальних схем та кримінальних бізнес-моделей або кримінального переслідування причетних до цього осіб, нейтралізації ОГ та ЗО, своєчасного виявлення та ефективного блокування джерел їхнього фінансування;
- аналіз наслідків впливу кримінальних загроз на суспільство, суспільні відносини та фінансово-економічну систему, з метою визначення заходів реагування на ризики, а також відвернення актуальних загроз та усунення вразливостей систем національної, економічної, публічної безпеки.

Принципами, які повинні бути покладені в основу такого підходу є:

- принцип безумовного пріоритету безпеки і збереження життя, здоров'я над будь-якими іншими елементами умов і якості життя членів суспільства;
- принцип прийнятного ризику (небезпеки), відповідно до якого встановлюються нижній (допустимий) і верхній (бажаний) рівні безпеки і в цьому інтервалі - прийнятний рівень ризику і безпеки з урахуванням соціально-економічних чинників;
- принцип мінімальної небезпеки, відповідно до якого рівень ризику встановлюється настільки низьким, наскільки він є реально досяжним;
- принцип послідовного наближення до абсолютної безпеки. [5]

У правоохоронних органах щодо застосування підходу на основі аналізу та оцінки ризиків принципи високого рівня і процедури, формуються на п'яти базових вимогах РОП:

1) розуміння загроз і вразливих місць, оцінка кримінальних ризиків;

2) наявність правової основи і правового регулювання для реалізації підходу;

3) розроблення базових механізмів нагляду за застосуванням РОП, що базується на оцінці ризиків суб'єктами контролю, а також реагуванням на ризики іншими власниками ризику;

4) ефективний розподіл обов'язків між суб'єктами контролю (іншими власниками ризику) і забезпечення взаємодії між ними;

5) обмін інформацією між державним і приватним сектором в частині оцінки ризиків національної, економічної, публічної безпеки, типологій та оцінки способів протиправного використання інструментів державного регулювання, фінансових інструментів та ін., особами, причетними до вчинення злочинів.

Набір інструментів окреслених РОП правоохоронних органів передбачає встановлення рівня ймовірності вчинення злочинів підслідних ним з огляду на існуючі кримінальні загрози (особа (група осіб), об'єкт або діяльність, що здатні завдати шкоди національній, економічній, публічній безпеці, суспільству) та вразливості (фактори, що створюють умови для виникнення кримінальних загроз) системи протидії злочинам у різних сферах, а саме шляхом:

а) раннього виявлення кримінальних загроз;

б) достовірної оцінки можливості їх реалізації;

в) встановлення вразливостей систем національної, економічної, публічної безпеки до кримінальних загроз;

г) оцінки наслідків та масштабів реалізації кримінальних загроз у співвідношенні із ідентифікованими вразливостями системи національної, економічної, публічної безпеки;

ґ) своєчасного усунення вразливостей системи національної, економічної, публічної безпеки;

д) запобігання негативним наслідкам прояву кримінальних ризиків;

е) визначення пріоритетних напрямів діяльності правоохоронних органів та інших інституцій забезпечення національної, економічної, публічної безпеки;

є) прийняття рішень про найбільш ефективне використання оперативних можливостей (ресурсів) правоохоронних органів.

РОП є одним з найважливіших інструментів для побудови ефективної програми протидії злочинності. Розуміння цих ризиків і пов'язаних з ними факторів надає змогу вживати більш ефективних і дієвих заходів з метою унеможливлення криміналізації системи суспільних відносин. Ризики мають динамічний характер, тому управління ризиками має здійснюватися безперервно. Необхідно, щоб присвоєні рівні ризику відповідали дійсно наявним ризикам, відображали реальну картину, і представляли ефективний метод оцінки.

Застосування показника ризику дозволяє порівнювати дію шкідливих та небезпечних чинників національної, економічної, публічної безпеки різної природи і різного виду, визначати з урахуванням внеску кожного окремого чинника інтегральний ступінь небезпеки будь-якого об'єкту, системи, технології, проекту, діяльності, процесу тощо. Проводячи порівняння ризиків, наприклад, пов'язаних з зайняттям підприємницькою діяльністю у неконкурентних умовах, з повсякденними кримінальними та корупційними ризиками, слід брати до уваги, що одні небезпеки приймаються суспільством добровільно (наприклад, оптимізація оподаткування), а інші - ні. Вельми важливо, що питання про сприйняття ризику істотно залежить від тих реальних вигод, які надає та або інша діяльність.

У контексті РОП слід виокремити наступні положення методик аналізу, оцінки та управління ризиками, застосування комплексу заходів з оцінки ризиків (- *далі КЗОР*):

Блок «оперативні можливості»

ОЦІНКА РИЗИКІВ

Правоохоронні органи повинні здійснити оцінку загроз організованої злочинності та тяжких злочинів (SOCTA), аналіз ризиків, а також разом з іншими суб'єктами контролю провести КЗОР відповідно до вимог діючого законодавства, особливо у разі якщо відповідно до вимог діючого законодавства вони визначені «національними координаторами». Наприклад, Національне антикорупційне бюро України може виступати «національним координатором» реалізації антикорупційної стратегії, Бюро економічної безпеки України - у забезпеченні економічної безпеки держави, Служба безпеки України - у забезпеченні національної безпеки, відповідно Національна поліція України - публічної безпеки тощо.

КМУ відповідно до діючого законодавства повинен призначити такі органи відповідальним за проведення КЗОР, з визначенням механізму координації такого заходу.

Національні координатори (визначені правоохоронні органи) за напрямом та інші суб'єкти контролю повинні регулярно здійснювати КЗОР з метою оновлення їх результатів.

Національні координатори повинні мати механізми комунікації за результатами проведення КЗОР з усіма суб'єктами контролю, зокрема правоохоронними органами та іншими суб'єктами державного регулювання.

УСУНЕННЯ РИЗИКІВ

Ґрунтуючись на власному розумінні своїх ризиків, суб'єкти контролю повинні застосовувати підхід, що ґрунтується на оцінці ризиків, при розподілі ресурсів та впровадженні заходів, спрямованих на запобігання та усунення ризиків національної, економічної, публічної безпеки.

Суб'єкти контролю, які приймають рішення не застосовувати деякі рекомендації КЗОР, у разі визначення їх власниками ризику, повинні продемонструвати, що:

(а) доведено низький рівень ризику національної, економічної, публічної безпеки; виняток має місце у суворо обмежених та обґрунтованих обставинах; та він стосується тільки певної категорії юридичних осіб, суб'єктів господарювання, розпорядників бюджетних коштів, отримувачів міжнародної технічної допомоги або діяльності, або

(б) фінансова (господарська) діяльність (окрім взаємовідносин з ОГ та ЗО) здійснюється фізичною або юридичною особою не регулярно або обмежено, процедури прийняття рішень та надання послуг суб'єктами контролю та суб'єктами державного регулювання транспарентні (беручи до уваги кількісний та абсолютний критерії), наприклад коли низький рівень ризику розкрадання бюджетних коштів та міжнародної технічної допомоги тощо.

Якщо національні координатори (визначені правоохоронні органи) за напрямом та інші суб'єкти контролю виявляють високі ризики, вони повинні забезпечити, щоб їхній режим забезпечення національної, економічної, публічної безпеки усував такі ризики, включаючи:

(а) встановлення вимоги до власників ризику вживати посилених заходів з управління та усунення ризиків, або

(б) встановлення вимоги до власників ризику забезпечувати, щоб ця інформація була включена в їхню власну систему оцінки ризиків.

Національні координатори (визначені правоохоронні органи) за напрямом та інші суб'єкти контролю можуть дозволити застосовувати спрощені заходи щодо деяких рекомендацій КЗОР, що встановлюють вимогу до власників ризику вживати певних заходів, за умови, що було визначено низький рівень, і це відповідає оцінці національного координатора у сфері відповідальності та іншими суб'єктами контролю своїх ризиків національної, економічної, публічної безпеки.

КМУ, РНБО та інші суб'єкти контролю повинні забезпечити, щоб усі суб'єкти державного регулювання, а також власне суб'єкти контролю виконували свої обов'язки відповідно до рекомендацій КЗОР, оцінки загроз організованої злочинності та тяжких злочинів (SOCTA), результатів аналізу ризиків, кримінального аналізу.

Блок «спроможність»

Ознаки спроможності системи: правоохоронні органи та інші суб'єкти контролю належним чином визначають, оцінюють та розуміють свої ризики національної, економічної, публічної безпеки, а також здійснюють координацію заходів на національному рівні, спрямованих на мінімізацію або уникнення ризиків, а у разі неможливості, пом'якшення наслідків або забезпечення відшкодування збитків у разі реалізації загрози. Це включає залучення компетентних органів та інших відповідних органів; використання широкого спектру надійних джерел інформації; застосування оцінки ризи-

ків як основи для розвитку та встановлення пріоритету стратегії та заходів з протидії злочинам; та впровадження цієї стратегії і заходів координованим шляхом через відповідні канали. Відповідні компетентні органи також співпрацюють та координують політику і заходи, спрямовані на діджитлізацію, зокрема системи надання публічних послуг, дозвільної та фіскальної систем тощо. З часом результатом цього стає значне пом'якшення ризиків національної, економічної, публічної безпеки.

Основні питання до розгляду при визначенні, чи досягнуто результат:

- ✓ *Наскільки вдало національні координатори та інші суб'єкти контролю усвідомлюють свої ризики національної, економічної, публічної безпеки?*
- ✓ *Наскільки вдало ідентифікуються ризики національної, економічної, публічної безпеки, що усуваються загальною стратегією забезпечення національної, економічної, публічної безпеки та заходами з протидії кримінальним загрозам?*
- ✓ *В якій мірі та чи належним чином використовуються результати аналізу та оцінки ризиків, факторів, що впливають на ризик, для обґрунтування винятків та підтримки застосування посилених заходів для випадків високого ризику або спрощених заходів для випадків низького ризику?*
- ✓ *В якій мірі цілі та заходи системи національної, економічної, публічної безпеки відповідають стратегіям забезпечення національної, економічної, публічної безпеки та протидії кримінальним загрозам, що розробляються, а також виявленим ризикам національної, економічної, публічної безпеки?*
- ✓ *В якій мірі національні координатори, інші суб'єкти контролю, громадські організації та суб'єкти підприємництва співпрацюють та координують розробку та впровадження стратегії і заходів, спрямованих на забезпечення прозорості фінансування виборчого процесу та політичних партій, оптимізації системи держуправління, а також спрощення процедур надання публічних послуг, детінізацію відносин в економіці та сфері управління публічними фінансами тощо?*
- ✓ *В якій мірі національні координатори та інші суб'єкти контролю забезпечують, щоб відповідні суб'єкти підприємництва, суб'єкти державного регулювання та надання публічних послуг, окремі юридичні та фізичні особи, а також інші учасники сектору забезпечення національної, економічної, публічної безпеки, були обізнані про відповідні результати КЗОР?*

Приклади корисної інформації для самооцінки роботи правоохоронного органу та інших суб'єктів контролю:

- ➢ Оцінка правоохоронними органами та іншими суб'єктами контролю своїх ризиків національної, економічної, публічної безпеки (наприклад, види здійсненої оцінки; види опублікованої/розповсюдженої оцінки);
- ➢ Концепції забезпечення національної, економічної, публічної безпеки та стратегії протидії кримінальним загрозам (наприклад, розповсюджені/опубліковані політики, стратегії та заяви з протидії кримінальним загрозам; залучення та зобов'язання вищих посадовців та політиків);
- ➢ Інформаційно-роз'яснювальна робота для приватного сектору та суб'єктів державного регулювання, органів влади (наприклад, брифінги та інструкції щодо відповідних висновків оцінки ризиків; частота та відповідність надання консультацій щодо усунення кримінальних та корупційних ризиків у законодавчих актах, внесок у розвиток аналізу, оцінки ризиків й управління ними, та інших політичних (управлінських) рішень).

Питання щодо факторів, які забезпечують досягнення результату національним координатором:

- *Які методи, інструменти, джерела та інформація використовується правоохоронним органом та іншими суб'єктами контролю з метою розробки, огляду та оцінювання результатів проведення КЗОР? Наскільки повною є інформація та дані, що використовуються?*
- *Наскільки релевантною є інформація до якої має доступ правоохоронний орган, а також цінними сам аналіз, а також методики, типології та підходи щодо прийняття управлінських рішень?*
- *Які суб'єкти контролю, інші компетентні органи та відповідні зацікавлені сторони (включаючи громадські організації, суб'єкти підприємництва, бізнес-асоціації тощо) залучені до аналізу, оцінки ризиків та управління ризиками? Який вони роблять внесок в КЗОР, і на якій стадії?*
- *Чи оновлюється оцінка ризиків та заходи реагування на ризики, чи регулярно вони переглядаються і чи відповідають вони значним подіям або змінам (включаючи нові загрози, інциденти, фактори впливу та тенденції)?*
- *В якій мірі аналіз й оцінка ризиків та управління ризиками є обґрунтованими та відповідають загрозам національної, економічної, публічної безпеки, слабким сторонам та можливостям суб'єктів забезпечення національної, економічної, публічної безпеки? За необхідності, чи враховують вони ризики, визначені іншими надійними джерелами?*
- *Чи відповідає політика правоохоронного органу та інших суб'єктів контролю на зміни ризиків національної, економічної, публічної безпеки?*
- *Який механізм(ми) використовуються правоохоронним органом для забезпечення належного та постійного співробітництва та координації системи забезпечення національної, економічної, публічної безпеки, а також для розробки та впровадження стратегії протидії кримінальним*

загрозам, як на рівні прийняття стратегічних управлінських рішень, так і на операційному рівні? Чи має правоохоронний орган, а також інші суб'єкти контролю оперативні можливості та необхідні повноваження для реагування на ризики?
- *Чи дозволяє існуючий механізм, від аналізу, оцінки ризиків до прийняття управлінських рішень щодо реагування на ризики, бути актуальним в питаннях забезпечення національної, економічної, публічної безпеки, вчасно здійснюється міжвідомчий обмін інформацією на двосторонній та багатосторонній основі?*
- *Чи існують відповідні ресурси та досвід для виявлення, аналізу, оцінки ризиків та управління ними, а також для співробітництва і координації між суб'єктами забезпечення національної, економічної, публічної безпеки?*

Основними джерелами первинної інформації правоохоронного органу є бази даних державних органів, зокрема контролюючих та інших правоохоронних органів, результати власної кримінальної розвідки та розслідувань кримінальних проваджень, Європол, OLAF, CARIN тощо. Елементами системи національної, економічної, публічної безпеки, які сприймають перероблену і надану правоохоронним органом інформацію у формі аналітичного продукту як стимул для виконання певної дії, є сукупність суб'єктів контролю (власників ризику), а також західні правоохоронні органи.

Мікрорівнева модель є фрактальною до макрорівневої, з урахуванням того, що функцію центрального фільтру в ній відіграють аналітичні підрозділи правоохоронного органу, а джерелами первинної інформації (у т.ч. генераторами ймовірних загроз) виступають (1) ОГ та ЗО, фактори, які сприяють криміналізації суспільних відносин (2) схеми та способи вчинення злочинів, а також способи відмивання злочинних доходів; (3) рішення, публічні процедури та послуги розпорядників бюджетних коштів тощо.

Таким чином, метою функціонування системи національної, економічної, публічної безпеки є подолання ситуації асиметричної поінформованості та інших вразливостей, які є генераторами загроз та ризиків, а також фасилітаторами використання кримінальних бізнес-моделей для вчинення злочинів.

Сутність ситуації з асиметричною поінформованістю полягає в тому, що нерідко суб'єкти контролю (учасники системи забезпечення національної, економічної, публічної безпеки) володіють нееквівалентною кількістю інформації про загрози, вразливості, наслідки, котрі є об'єктом інтеракцій (тобто безпосередня міжвідомча взаємодія, найважливішою особливістю котрої визнається здатність однієї структури «приймати на себе роль іншої»). Це означає, що окремі суб'єкти контролю, що задіяні в системі забезпечення національної, економічної, публічної безпеки мають інформаційну перевагу над іншими, що об'єктивно і неминуче ускладнює прийняття учасниками системи оптимального управлінського рішення.

Порядок пріоритетів при розробці будь-яких Стратегій розвитку вимагає, щоб вже на перших стадіях їх розробки або побудови системи національної, економічної, публічної безпеки, наскільки це можливо, були включені елементи, що мінімізують ризики вчинення кримінальних, зокрема корупційних, правопорушень. На жаль, це не завжди можливо. Якщо ідентифіковану загрозу неможливо відвернути повністю, необхідно знизити ймовірність ризику до прийнятного рівня шляхом вибору відповідного рішення. Досягти цієї мети, як правило, в будь-якій системі чи ситуації можна кількома шляхами:
- *усунути джерело ризику, наприклад нейтралізувати вплив організованих груп та злочинних організацій;*
- *використовувати штучний інтелект з метою моніторингу загроз, прогнозування ризику та превентивного впливу на загрози;*
- *підвищити спроможність державних інституцій з мінімізації ризиків, розробити концепцію (структури) ризик-менеджменту, процесу управління ризиками, проводити моніторинг виконання необхідних дій, постійно вдосконалювати ризик-менеджмент;*
- *застосовувати заходи організаційно-управлінського характеру, інтегрувати політику ризик-менеджменту в загальну політику правоохоронного органу, встановити відповідальності та повноваження «власників ризиків» в системі ризик-менеджменту, запровадити протоколи ідентифікації ризику, формувати в такому ключі кадрову політику тощо.*

Як правило, для підвищення рівня національної, економічної, публічної безпеки завжди використовується комплекс цих заходів та засобів. Для того щоб надати перевагу конкретним заходам та засобам або певному їх комплексу, порівнюють витрати на ці заходи та засоби і рівень зменшення шкоди, який очікується в результаті їх запровадження.

Такий підхід до зменшення ризику зветься управління ризиком - *це розроблення, на основі оцінювання ризиків, та реалізація управлінських рішень, спрямованих на мінімізацію таких ризиків, а також на підвищення спроможності державних інституцій щодо нейтралізації загроз національної,*

економічної, публічної безпеки. З метою підвищення рівня безпеки, інституціональної спроможності суб'єктів контролю зусилля треба спрямовувати за трьома напрямами:

а) надання достатніх юридичних повноважень та людських ресурсів, удосконалювання технічних систем та оперативних можливостей;

б) підвищення рівня компетентностей (підготовка кадрів);

в) ліквідація наслідків у разі неможливості відвернути загрозу.

Враховуючи вищезазначене можна сформувати правила ризик-менеджменту національної, економічної, публічної безпеки, що забезпечується в межах компетенції правоохоронним органом:

> *реагувати на ризики в межах інституціональних можливостей правоохоронного органу, а також інших суб'єктів контролю;*
>
> *враховувати наслідки ризику будь-якого втручання в систему публічних або суспільних відносин;*
>
> *втрати у разі реалізації загрози національної, економічної, публічної безпеки повинні співвідноситись з витратами на її долання або мінімізацію. Модель індексу витрат, що очікуються базується на вартості витрат у системі порівняно з вірогідністю втрат. Індекс втрат, що очікуються, у разі свідомого не реагування на ризик або відсутності можливості такого реагування;*
>
> *мати декілька варіантів впливу на ризики національної, економічної, публічної безпеки: або використовувати інструменти превентивного впливу або кримінального переслідування;*
>
> *приймати рішення щодо впливу на ризик лише у разі відсутності сумніву.*

Іншим аспектом того, як встановлюється співвідношення витрат з розміром прийнятного ризику, є можливість контролю чи мінімізації ризику. Деякі загрози, що мають відносно низький рівень ризику, вважаються неприпустимими, тому що їх досить легко контролювати та відвернути.

Навпаки, існують інші загрози, які вважаються допустимими, хоча мають значний потенціал ризику, через те що їх важко або практично неможливо відвернути. Отже, вартість не є єдиним та головним критерієм встановлення прийнятного ризику. Важливу роль відіграє оцінка процесу, вона пов'язана з виявленням та оцінкою ризику.

Заходи, що вживаються правоохоронним органом на основі РОП, наприклад, стосовно ОГ та ЗО - симулякру, що зорієнтовано на суто кримінальну економічну діяльність або надання кримінальних послуг суб'єктам реального сектору економіки становлять високий ризик, повинні бути пропорційними виявленим ризикам та спрямовані на їх мінімізацію, у тому числі шляхом збільшення частоти та обсягу дій з моніторингу фінансово-господарської діяльності та діяльності суб'єктів контролю та збору додаткової інформації, у тому числі оперативним шляхом.

КОМПЛЕКС ЗАХОДІВ З ОЦІНЮВАННЯ РИЗИКІВ (КЗОР)

З метою побудови ефективної системи стратегічного менеджменту в забезпеченні національної, економічної, публічної безпеки на середньострокову перспективу, визначенні місця ОГ та ЗО і способів кримінальних проявів у загальному переліку ідентифікованих загроз, вразливостей / спроможностей системи національної, економічної, публічної безпеки, РОП також супроводжується проведенням КЗОР. Організовує такий захід національний координатор у сфері (уповноважений правоохоронний орган) із залученням державних органів, громадських організацій, бізнесу та інших, що опікуються питаннями національної, економічної, публічної безпеки та інших експертів (у разі потреби). КЗОР повинен проводитись систематично, але не рідше одного разу на три роки. Такий комплекс заходів сприяє визначенню місця кожного суб'єкта контролю, в системі забезпечення національної, економічної, публічної безпеки. У такому випадку уповноважений правоохоронний орган виступає своєрідним «Національним координатором» систем забезпечення національної, економічної, публічної безпеки.

Виходячи із зазначеного вище, та з урахуванням результатів опрацювання перелічених вище методологічних джерел, цілі проведення КЗОР можна конкретизувати через сукупність наступних завдань:

- *зниження ймовірності виникнення ризику національної, економічної, публічної безпеки та ризику вчинення кримінальних правопорушень;*
- *оцінка ступеня загрози реалізації ризику національної, економічної, публічної безпеки та ризику вчинення кримінальних правопорушень;*
- *оцінка ступеня вразливості системи національної, економічної, публічної безпеки відносно актуальних загроз та ризику вчинення кримінальних правопорушень;*

- *співвіднесення ступеня кримінальної загрози реалізації ризику та потенційних наслідків його прояву із обсягом ресурсів, які спрямовуються на зниження відповідного ризику;*
- *мінімізація наслідків за умови реалізації ризику національної, економічної, публічної безпеки та ризику вчинення кримінальних правопорушень.*

Звіт, який формується за результатами проведення КЗОР, є необхідною передумовою для уповноважених суб'єктів забезпечення національної, економічної, публічної безпеки в контексті розробки і запровадження ефективної Стратегії, тобто визначення пріоритетів у політиці забезпечення національної, економічної, публічної безпеки та ризик-орієнтовану пріоритезацію щодо розподілу ресурсів.

Система оцінювання ризиків представляє інформацію для національного координатора та інших суб'єктів контролю (власників ризику), яка дозволяє зрозуміти, чи відповідає чинне законодавство цілям реалізації превентивного впливу на нові загрози національної, економічної, публічної безпеки і чи достатніми є оперативні можливості, юридичні повноваження та компетентності зазначених органів.

Методологія РОП щодо аналізу, оцінки ризиків та управління ними в питаннях протидії кримінальним загрозам та забезпечення національної, економічної, публічної безпеки ***базується на п'яти принципах***, а саме:

1) розуміння загроз і вразливих місць системи національної, економічної, публічної безпеки, а також оцінки кримінальних ризиків;

2) визначення законодавчої процедури для реалізації підходу;

3) розроблення базових механізмів роботи національного координатора системи забезпечення національної, економічної, публічної безпеки щодо нагляду за способами реагування на ризики суб'єктами контролю, що базується на оцінці ризиків;

4) ефективний розподіл ризиків між власниками ризику (суб'єктами контролю) і забезпечення координації дій між ними в питаннях уніфікації підходів щодо оцінки ризиків та способів (інструментів) реагування на ризики;

5) обмін інформацією між державним сектором, бізнесом та суспільством в частині оцінки ризиків, типологій та оцінки способів протиправного використання різних форм підприємництва та фінансової системи особами, причетними до протиправної діяльності.

Ранжування принципів КЗОР здійснюється наступним чином:

1) Узгодження цілей і масштабів КЗОР

У якості цілей оцінки ризиків можуть виступати:

- оцінка характеру і масштабів криміналізації суспільних відносин, виявлення факторів, які сприяють такій криміналізації, оцінка спроможностей правоохоронної інституції у протидії конкретним кримінальним загрозам, причини виникнення попиту на кримінальні послуги на тіньовому ринку, оцінка життєвого циклу кримінальних схем та діяльності ОГ та ЗО, як загрози тощо. Вказана оцінка полягає у виявленні відсотка учасників суспільних відносин певної сфери та ресурсів, задіяних у кримінальних оборудках, а також в ідентифікації способів, схем вчинення кримінальних правопорушень, з урахуванням результативності роботи уповноваженого правоохоронного органу, як національного координатора, інших правоохоронних та контролюючих органів, а також з урахуванням притягнення до відповідальності правопорушників і винесення судових вироків;
- визначення конкретних продуктів, послуг, управлінських рішень, видів діяльності, сфер, галузей, які є найбільш вразливими до ризиків національної, економічної, публічної безпеки;
- виявлення слабких сторін (вразливостей) системи національної, економічної, публічної безпеки, а також інших особливостей щодо функціоналу, обмеженістю юридичних повноважень чи компетенцій, які роблять її привабливою для правопорушників;
- розробка Стратегій забезпечення національної, економічної, публічної безпеки та заходів щодо їх реалізації;
- розподіл ресурсів між суб'єктами контролю (власниками ризику) тобто уповноваженими учасниками системи національної, економічної, публічної безпеки, наприклад між правоохоронними органами, державними регуляторами, зокрема контролюючими органами.

Цілі та масштаби КЗОР можуть відрізнятися і залежати від багатьох вхідних управлінських рішень. На масштаби оцінки, зокрема, може вплинути рішення про те, чи проводиться КЗОР диференційовано для протидії конкретним правопорушенням у сфері економіки або управління публічними фінансами чи в комплексі, наприклад, для забезпечення економічної (фінансової, інвестиційної, фіскальної тощо) безпеки держави. З іншого боку, цілі і масштаби КЗОР залежать від потреб корис-

тувачів (виконавчої, законодавчої влади, регулюючих і правоохоронних органів, бізнес-спільноти, громадськості, науково-експертних установ тощо) і тому мають бути узгодженими із зацікавленими сторонами, виконавцями і користувачами результатів КЗОР.

2) Комплексність КЗОР

Оцінка ризиків на національному рівні нерозривно зв'язана з їхньою оцінкою на рівні конкретних сфер життєдіяльності, секторів економіки, управління публічними фінансами, галузей, видів економічної діяльності, продуктів, алгоритмів роботи окремих державних інституцій та бізнесу, специфіки регіонів країни. Вказане обумовлює реалізацію принципу комплексності оцінки. Таку комплексність можна визначити як можливість зведення (узагальнення) результатів всіх окремих оцінок і формування цілісної картини ризиків.

> *Комплексність передбачає наявність єдиного підходу до застосування РОП та КЗОР, використання єдиної інформаційної бази (єдиної бази статистичних показників), системний підхід до збору кількісних даних щодо протидії кримінальним правопорушення.*

Оцінки, одержані щодо різних сфер життєдіяльності, видів економічної діяльності, секторів економіки, управління публічними фінансами та надання публічних послуг, галузями, продуктами, способами та характером ведення господарської діяльності, у сумі повинні давати загальну оцінку ризиків національної, економічної та публічної безпеки. Оцінки уповноваженого правоохоронного органу та інших суб'єктів контролю у сфері протидії кримінальним правопорушенням мають бути співставними. У той же час, при здійсненні КЗОР, основні зусилля слід зосередити на оцінці тих ризиків, які впливають на всі системи національної, економічної, публічної безпеки.

3) Політична воля, зобов'язання виконавчої та законодавчої влади щодо РОП та КЗОР

Політична воля в такому контексті визначається як зобов'язання вищих органів виконавчої влади щодо проведення КЗОР, а також розуміння такими особами наявності відповідних ризиків національної, економічної, публічної безпеки. РОП та КЗОР не повинні залежати від конкретного політичного курсу і законодавчих реформ, а також від лобіювання з боку зацікавлених осіб.

4) Організація взаємодії органів, залучених до проведення КЗОР у сфері протидії кримінальним правопорушенням

Учасниками КЗОР є:
- *органи виконавчої влади;*
- *Уповноважений правоохоронний орган та інші правоохоронні органи;*
- *спецслужби;*
- *контролюючі органи та органи регулювання і нагляду;*
- *громадські організації та бізнес асоціації;*
- *представники бізнес-середовища;*
- *представники науково-експертного дослідницького середовища.*

Важливу роль в оцінці ризиків відіграють контролюючі органи, державні регулятори, органи державного фінансового контролю, підрозділи фінансового моніторингу, які мають справу із контролем, адмініструванням, моніторингом фінансових операцій та бізнес-процесів, контролем за використанням і збереженням державних фінансових ресурсів. Такі структури виявляють осіб, процеси, об'єкти та події, які відносяться до групи підвищеного ризику, а також з'ясовують характер зв'язків (зокрема ділових), управлінських рішень та послуг з відповідними ризиками. уповноважений правоохоронний орган та інші правоохоронні органи розробляють систему статистичних показників – критерії для оцінювання ризиків. Крім того уповноважений правоохоронний орган забезпечує координацію дій із реагування на ризики у процесі забезпечення національної, економічної, публічної безпеки.

У виявленні і оцінці ризиків надзвичайно важливою є міжнародна взаємодія в контексті обміну інформацією і використання набутого досвіду. Уповноважений правоохоронний орган здійснює співробітництво з компетентними органами інших держав, міжнародними, міжурядовими організаціями в межах своєї компетенції відповідно до законодавства України та міжнародних договорів України. Працівники правоохоронного органу можуть направлятися до міжнародних організацій, іноземних держав як компетентні представники з метою забезпечення координації співробітництва з питань, що належать до повноважень правоохоронного органу, та залучаються до участі в міжнародних заходах, пов'язаних із забезпеченням національної, економічної, публічної безпеки, а також міжнародних заходах з обміну досвідом.

Правоохоронний орган здійснює міжнародне співробітництво, спираючись як на двосторонню, так і з багатосторонню взаємодію.

Двостороння взаємодія реалізується виходячи із міжвідомчих, міжурядових та міждержавних угод.

Багатостороння взаємодія спрямована на:

- *розроблення та удосконалення стандартів РОП, у т.ч. підходів щодо протидії кримінальним правопорушенням;*
- *на імплементацію цих стандартів у правоохоронну практику та законодавчого регулювання системи досудового розслідування та кримінальної розвідки, а також превентивної діяльності.*

Багатостороння взаємодія реалізується в рамках рекомендацій та документів Організації економічного співробітництва та розвитку (ОЕСР), Оцінки загроз з боку особливо небезпечних форм організованої злочинності (SOCTA (оцінка загроз організованої та серйозної злочинності), IOCTA (кіберзагрози), TE-SAT (терористичні загрози), інших міжнародних аналітичних оглядів, звітів та рекомендацій з питань, пов'язаних з проведенням КЗОР.

5) Наявність координуючого органу з питань проведення КЗОР.

Значна кількість учасників, які залучаються до проведення КЗОР, передбачає наявність координуючого органу для управління збором, обробкою і аналізом інформації з метою виявлення (актуалізації) кримінальних ризиків (загроз, вразливостей, наслідків) в системі забезпечення національної, економічної, публічної безпеки, визначення елементів управління ними та сприяння у розробці стратегії розвитку систем національної, економічної, публічної безпеки, а також для підготовки кінцевого документу про оцінку ризиків.

Відповідальним за проведення КЗОР повинен бути уповноважений правоохоронний орган.

6) Гнучкість (актуалізація, розвиток) системи РОП та КЗОР

Гнучкість системи передбачає можливість її коригування і розвитку з урахуванням нових загроз та вразливостей, які виникають. Розвиток пов'язаний насамперед із постійним удосконаленням методики оцінки ризиків, а також підходів, способів та заходів реагування на ризики, із включенням у вхідну інформаційну базу нових джерел статистичних даних, всебічним аналізом результатів КЗОР в динаміці, виявленням тенденцій, які виникають а також множинних регресійних взаємозв'язків між сукупністю статистичних даних на яких базуються емпіричні висновки КЗОР.

КЗОР проводиться систематично, але не рідше одного разу на три роки. Останній рік звітного періоду є роком проведення КЗОР.

7) Поєднання кількісної і якісної вхідної інформації, її достатність і різнобічність

Якість КЗОР в значній мірі залежить від виду і якості наявної статистики, різноманітних даних (ретроспективних і перспективних, кількісних і якісних, а також комбінованих), якості процедур збору даних в рамках систем національної, економічної, публічної безпеки. Кількісні оцінки, які базуються на статистичних даних є більш надійними. Часові ретроспективні ряди динаміки дозволяють прогнозувати тенденції і майбутні проблеми.

Показники, що розраховані на основі кількісних даних, дозволяють не тільки підтвердити ідентифіковану експертами якісну оцінку загроз і вразливостей, але й глибше розглянути компоненти систем забезпечення національної, економічної, публічної безпеки, виміряти їх, порівняти і розставити пріоритети.

Серед інших даних, до кількісних оцінок системи протидії кримінальним правопорушенням відноситься статистика по кримінальному судочинству і суми відшкодованих збитків або упереджених втрат бюджету за рахунок застосування превентивних заходів впливу, а також дані по оперативним можливостям (ресурсах), компетентностям, юридичним повноваженням, які задіяні уповноваженим правоохоронним органом та іншими суб'єктами контролю в системі протидії злочинам, про наявність кримінального попиту та пропозицій на тіньовому ринку на кримінальні бізнес-моделі та рівень втягуваності суб'єктів підприємництва у тіньові процеси, суми коштів, задіяних у тіньовому обігу, рівень загрози життю та здоров'ю населення тощо.

Інструментарієм збору кількісних даних можуть виступати матриці (шаблони), приклади яких, наведені у Методологіях проведення аналізу ризиків та управління ризиками, методиках проведення кримінального аналізу, а також додаткові критерії, які використовуються у процесі проведення КЗОР і SOCTA та оцінки стійкості систем національної, економічної, публічної безпеки.

Важливість врахування вищевказаних критеріїв з Методології проведення аналізу ризиків полягає у тому, що вона є основним робочим документом, який використовується уповноваженим правоохоронним органом та іншими суб'єктами контролю при проведенні взаємних оцінок. У свою чергу, мета взаємних оцінок полягає у формуванні ефективних систем національної, економічної, публічної безпеки.

Звіти уповноваженого правоохоронного органу повинні містити докладні рекомендації з питань зміцнення стійкості систем національної, економічної, публічної безпеки, підвищення ефектив-

ності протидії кримінальним правопорушенням, а також використання спроможностей суб'єктів контролю реагувати на ризики.

8) Документальне оформлення інструментарію і результатів КЗОР

Документальне оформлення методики, алгоритмів, процедур КЗОР, а також інформації, яка містить результати аналізу ризиків та висновки, необхідне для інформування всіх учасників КЗОР, як власників ризику про зони компетенцій з оцінки ризиків та реагування на ризики, для забезпечення транспарентності процедур, виявлення динаміки і тенденцій в оцінці ризиків. Аналітичний продукт є базою для прийняття рішень експертами з аналізу ризиків національної, економічної та публічної безпеки та протидії кримінальним правопорушенням.

ЦИКЛ РОП ЩОДО ЗАБЕЗПЕЧЕННЯ ПУБЛІЧНОЇ БЕЗПЕКИ І ПОРЯДКУ, ПРОТИДІЇ ЗЛОЧИННОСТІ

Побудова концептуальної моделі забезпечення національної, економічної та публічної безпеки можлива лише на основі вибору науково обґрунтованого переліку кількісних показників, які є індикаторами ризиків і сигналізують про посилення вірогідності (наближення часу) виходу криміногенної ситуації за межі контрольованої. При цьому мають значення не самі показники, а їх відхилення від порогових рівнів. Порогові значення індикаторів ризиків – це такі граничні величини, наближення до яких сигналізує про зниження рівня національної, економічної та публічної безпеки, збільшення кількості вчинення кримінальних правопорушень, а перевищення граничних, або порогових, значень – про настання неконтрольованої ситуації. Вибір показників залежить від тривалості періоду, протягом якого потрібно оцінити ризики та виявити загрози національної, економічної та публічної безпеки. В контексті зазначеного потребує зміни підходів до вивчення явищ, зокрема шляхом його оцифровування у спосіб, що забезпечує можливість його аналізу за допомогою штучного інтелекту.

З тим щоб досягти мети з мінімізації ризику правоохоронний орган розробляє шкалу ризиків, яка містить відповідні фактори ризику. Отже, самі ризики, їх аналіз та оцінка, заходи з реагування на ризики повинні переглядатися та оновлюватися правоохоронним органом у випадках зміни факторів ризику.

Цикл РОП щодо забезпечення національної, економічної та публічної безпеки включає наступні дії:

1) виявлення джерел ризику та факторів впливу за яких виникає ризик, ідентифікація всіх можливих ризиків національної, економічної та публічної безпеки;

2) оцінка рівня окремих ризиків національної, економічної та публічної безпеки та втрат (шкоди), що очікуються, у разі не реагування на ризик або відсутності можливості такого реагування;

3) визначення прийнятного рівня ризику;

4) розробка та вжиття заходів з мінімізації ризику;

5) оцінка підходів та заходів з мінімізації ризику.

Крок 1: виявлення джерел ризику та факторів впливу, за яких виникає ризик, ідентифікація всіх можливих ризиків національної, економічної та публічної безпеки.

Для ефективної оцінки кримінальних ризиків їх можливо поділити на дві частини:

1. Оцінка ризиків, притаманних певним сферам життєдіяльності, а також певним процесам, публічним послугам (ризик-профіль правопорушника або правопорушення): за ризиковістю самого суб'єкта, ризиковістю діяльності, ризиковістю зв'язків та іншими відповідними факторами.

2. Оцінка вразливостей суб'єктів контролю, тобто учасників системи забезпечення національної, економічної та публічної безпеки (ризик-профіль «недобросовісного контролера»): інструменти, повноваження, послуги, які використовуються для сприяння криміналізації суспільних відносин, бездіяльність суб'єктів контролю в усунення вразливостей або впливі на загрозу, географічні місця або ієрархічний рівень прийняття рішень, компентентності працівників, наявність оперативних можливостей, а також статус інституції та характер її повноважень в системі забезпечення національної, економічної та публічної безпеки тощо.

Визначення ризиків, притаманних національній, економічній та публічній безпеці, вимагатиме від правоохоронного органу розглядати вразливості таких систем. Правоохоронний орган розпочинає оцінку ризику із загального огляду системи суспільних відносин, галузей економіки, процесів з державного регулювання або надання публічних послуг тощо. Це дозволяє визначити, де виникають ризики, пов'язані з різними напрямами жтттєдіяльності, адміністрування податків, державного регулювання, надання публічних послуг, управління публічними фінансами, інструментами або конкретними продуктами.

Сфери, віднесені до категорії високого ризику, повинні мати документовані стратегії з мінімізації ризиків. Для того, щоб встановити вразливість системи національної, економічної та публічної безпеки до впливу криміногенних факторів на неї та ефективне управління цим ризиком, правоохоронному органу необхідно ідентифікувати кожен сегмент соціальних та бізнес процесів (операцій), системи адміністрування податків, надання публічних послуг та/або управління публічними фінансами тощо де може виникнути кримінальна загроза, і оцінити вразливість системи до цієї загрози.

Кримінальні ризики національної, економічної та публічної безпеки повинні постійно виявлятися правоохоронним органом на всіх рівнях управління і включати всі структурні одиниці задіяні в цій системі. Розмір і складність бізнес-процесів, процедур публічних послуг та транспарентність управлінських рішень, відіграють важливу роль у тому, наскільки вони привабливі або сприйнятливі до криміналізації. Після визначення кримінальних ризиків правоохоронний орган повинен адекватно оцінити схильність до ризику певної сфери життєдіяльності, зокрема економічної та/або бюджетної сфери, що дозволить йому оцінити ймовірність несприятливих наслідків, пов'язаних з цим ризиком, і потенційний вплив цього ризику на суспільство, здоров'я людини, реалізацію нею своїх прав, а також на підприємництво або втрати бюджету.

Ідентифікація та аналіз ризиків повинні проводитися для всіх наявних і нових продуктів, нових видів діяльності, публічних процедур і процесів, визначення нових суб'єктів контролю або зміни їх повноважень. Ефективний процес виявлення та аналізу кримінальних ризиків є основою для створення адекватної системи управління ризиками та контролю за ними і, отже, для досягнення кінцевої мети - мінімізації можливих несприятливих наслідків, що виникають у результаті цього ризику.

Метою оцінки ризику є застосування заходів контролю, пропорційних виявленому ризику. Це дозволяє правоохоронному органу зосередитися на фігурантах, країнах, публічних процедурах, видах діяльності, продуктах і послугах та способах їх надання, попиті та пропозиціях на схеми на тіньовому ринку, які представляють собою найбільший потенційний ризик.

Одним з найважливіших факторів при розробці шкали ризиків є географічний ризик, який відображає взаємозалежність місця вчинення кримінального правопорушення, місця побудови кримінальної інфраструктури та місце розташування «недобросовісного контролера» або його ієрархічний рівень.

Оцінюючи таку географічну локацію правоохоронний орган повинен враховувати, чи представляє така взаємозалежність потенційно високий ризик національної, економічної та публічної безпеки.

При визначенні ризик-профілю правопорушника та/або «недобросовісного контролера» доцільно враховувати й інші фактори ризику, зокрема:

- *елементи ризиків, маркери та індикатори вчинення кримінального правопорушення (червоні прапорці);*
- *операційна структура суб'єктів забезпечення національної, економічної та публічної безпеки їх оперативні можливості та юридичні повноваження, компетентність, кількість відділень, філіалів та співробітників;*
- *здійснення практичної діяльності з високою плинністю кадрів суб'єктів контролю, тощо.*

Після того, як правоохоронний орган визначив та задокументував усі притаманні ризики, їм потрібно присвоїти рівень для кожного ризику. Необхідно встановити шкалу ризику з урахуванням розміру та типу діяльності.

Аналітики та детективи повинні знати і розуміти наявні ризики національної, економічної та публічної безпеки на національному, регіональному та секторальному рівнях. При оцінці ризиків повинні враховуватися результати КЗОР, Оцінювання загроз організованої злочинності у сфері економіки (SOCTA), рекомендацій ОЕСР, а також Типологічні дослідження правоохоронних органів відповідно до визначеної компетенції та інших доступних джерел.

Оцінка ризиків розробляється на основі характеристик, притаманних сфері життєдіяльності, виду публічних послуг, публічним процедурам, суб'єкту господарювання, виду підприємництва, способу та формам фінансово-економічної діяльності, членів ОГ та ЗО, функціоналу та повноваженням суб'єктів контролю.

Індикатори високого ризику

Рішення про присвоєння рівня ризику суб'єкта/публічних послуг, рішень/ділових відносин (події, інциденту) має прийматися на підставі мотивованого аналітичного судження, сформованого у процесі аналізу наявної інформації про суб'єкта (члена ОГ та ЗО, розпорядника бюджетних коштів, суб'єкта надання публічних послуг, власника бізнесу, вигодонабувача, кінцевого бенефіціарного власника, недобросовісного контролера тоощо), подій (ділових відносин, інцидентів), а також оперативних відомостей, отриманих за результатами проведення агентурних операцій, інших НСРД

(оперативно-розшукових заходів), відповідно до внутрівідомчих нормативних актів, та інших внутрішніх документів з питань проведення аналізу ризиків, матеріалів кримінальних проваджень, у тому числі інформації щодо:

- криміногенних процесів, господарських/виробничих, бюджетних, фіскальних процесів, інструментів вчинення злочинів, часових інтервалів (частоти застосування) та визначення причинно-наслідкових зв'язків, втягуваності.
- еволюції загальної кількості інцидентів, зафіксованих за певний проміжок часу, порівняно з аналогічними періодами попередніх років;
- динаміки спричинених збитків, втрат бюджету (податкових надходжень та/або освоювання бюджетних коштів), кількості жертв / інцидентів за аналізований період;
- сфери, географічного розташування, місця виникнення інцидентів та / або жертв, секторів та місць втрат бюджету;
- середнього значення інцидентів та / або жертв, сум втрат бюджету у визначений проміжок, а також за сферою та місцем виникнення;
- часових інтервалів, в яких відбуваються інциденти;
- існування та впливу зовнішніх економічних, соціальних та географічних факторів;
- фінансового профілю суб'єкта, який перевіряється;
- результатів виявлення серед суб'єктів, які перевіряються політично-значущих осіб та пов'язаних з ними осіб. Рекомендується також проводити перевірку кінцевого бенефіціарного власника суб'єкта, що перевіряється, з метою виявлення вищезгаданих осіб;
- встановлення взаємозв'язку між інцидентами, що аналізуються, та діями осіб (фізичних, юридичних), які знаходяться на оперативному обліку або відносно яких є інформація про причетність до протиправної діяльності;
- інших відомостей, які самостійно визначаються правоохоронним органом.

«Недобросовісні контролери» потенційно представляють підвищений ризик, тому що мають можливості зловживати впливом на прийняття рішень, що стосуються способів реагування на ризики публічної безпеки, фінансово-господарської діяльності приватного сектора або мають доступ до прийняття рішень у економічній, публічно фінансовій, зокрема фіскальній сферах.

Правоохоронний орган може використовувати матрицю ризику як метод оцінки ризику для визначення типів або категорій суб'єктів, процесів, явищ, які знаходяться в зоні низького ризику, тих, які становлять дещо вищий, але все ще прийнятний ризик, і тих, які становлять високий або неприйнятний ризик вчинення кримінального правопорушення. При класифікації ризику суб'єкти контролю, враховуючи свої особливості, можуть також визначити додаткові рівні ризику. Розробка матриці ризиків може включати розгляд широкого спектру категорій ризиків, таких як продукти, публічні процедури, сформований попит та пропозиції на кримінальні бізнес-моделі, споживачі, яким пропонуються продукти і кримінальні послуги, компетенція та юридичні повноваження та організаційна структура суб'єктів контролю тощо. Матриця ризику не є статичною: вона змінюється в залежності від зміни обставин у сфері життєдіяльності.

Крок 2: оцінка рівня окремих ризиків національної, економічної та публічної безпеки та втрат, що очікуються, у разі не реагування на ризик або відсутності можливості такого реагування.

Визначення і оцінка ризиків, тобто визначення ймовірності виникнення ризику і наслідків у разі прояву ризику та реалізації загрози національній, економічній та публічній безпеці. При оцінці ризику, необхідно визначити найбільш вразливі місця систем національної, економічної та публічної безпеки, які впливають на спроможність суб'єктів контролю відвернути кримінальну загрозу. Виявлені ризики можуть змінюватися або розвиватися з часом, коли нові продукти або нові загрози з'являються у системі суспільних відносин та потраплять у поле зору правоохоронного органу.

Критерії ризиків визначаються правоохоронним органом самостійно з можливим урахуванням критеріїв ризиків контролюючих органів.

Правоохоронний орган в межах повноважень повинен отримати право вживати відповідні превентивні заходи для мінімізації ризиків, на усунення причин, умов, чинників, які сприяють вчиненню кримінальних правопорушень, а також мінімізації ризиків, що сприяють криміналізації процесів у сфері суспільних відносин, зокрема економіці та управління публічними фінансами. *Правоохоронний орган зобов'язаний встановити високий ризик ділових відносин стосовно ОГ та ЗО, зокрема якщо така група:*

- *має більш ніж 9 членів;*
- *ієрархічно структурована із внутрішніми системами розподілу ролей, контролю та порядку;*
- *«професійне», яке мімікрує під різні бізнес утворення або види господарської діяльності або надає кримінальні послуги представникам реального сектору економіки;*
- *цілеспрямовано діє в інтересах країни-агресора;*

- *діє на тимчасово непідконтрольних (анексованих) територіях;*
- *здійснює свою діяльність на транснаціональному рівні;*
- *володіє значними фінансовими ресурсами для своєї злочинної діяльності або може легко знайти такі ресурси;*
- *вчинює злочин як кримінальну послугу для інших учасників кримінального ринку та/або використовує досвідчених/висококваліфікованих фахівців або складні технічні інструменти на постійній основі;*
- *стратегічно здійснює свою діяльність на різних кримінальних ринках, які не взаємопов'язані між собою;*
- *є повністю незалежним або співпрацює з іншими ОГ та ЗО та є домінуючим у спільній діяльності;*
- *є «новатором» і довело, що активно шукає нові можливості на легальних та нелегальних ринках. ОГ та ЗО є гнучким, швидко та креативно пристосовується до змін зовнішнього середовища;*
- *часто відмиває велику кількість доходів від протиправної діяльності із використанням складних та інноваційних схем або основним видом діяльності якої є надання послуг з відмивання доходів для інших ОЗУ;*
- *має спеціалізацію, для реалізації якої необхідно створення розгалуженої кримінальної інфраструктури;*
- *створює власні СГ або проникає в існуючі СГ на високому рівні або може вступити у змову з керівниками високого рівня цих суб'єктів;*
- *має добре розуміння методів діяльності правоохоронних органів і стратегічно використовує інноваційні заходи протидії;*
- *використовує насильство та/або залякування в агресивний, спланований, обміркований спосіб та/або насильство є непропорційним загрозі його діяльності;*
- *часто й активно користується корумпованими зв'язками з державними службовцями категорії «А»;*
- *володіє значним арсеналом зброї;*
- *під час вчинення тяжких злочинів систематично використовуються транснаціональні зв'язки з мешканцями (злочинцями), юридичними особами з трьох і більше країн тощо.*

Тобто при присвоєнні високого рівня ризику оцінюється: рівень можливостей ОГ та ЗО отримувати та використовувати фінансові ресурси; полікримінальна діяльність (індикатор діяльності ОГ та ЗО у різних злочинних сферах для збільшення незаконних доходів та зменшення ризиків); використання ОГ та ЗО осіб із спеціальними навичками й знаннями та/або специфічних засобів і технологій для полегшення протиправної діяльності; індикатори спроможності ОГ та ЗО використовувати легальні бізнес-структури, СГ – суб'єкти господарювання; адаптивність та гнучкість (можливість ОГ та ЗО пристосовувати свою злочинну діяльність до змін у зовнішньому середовищі для використання легальних та нелегальних ринків); здатність ОГ та ЗО відмивати доходи від протиправної діяльності і рівень складності методів їх діяльності, починаючи від високопродуктивних механізмів; кримінальна інфраструктура (індикатор спроможності ОГ та ЗО забезпечити довготривале функціонування технологій, схем та способів вчинення злочинів); фактори, які впливають на сферу злочинної діяльності; співвідношення між попитом і пропозицією на незаконні товари/послуги у цій сфері злочинної діяльності; вплив сфери злочинної діяльності на зовнішнє середовище тощо.

Крок 3: визначення прийнятного рівня ризику.

Концепцією аналізу ризиків в питаннях управління безпекою є порівняння поточного ризику з припустимим (прийнятним), зроблені на підставі цього відповідні висновки та прийняті до виконання рішення, а методологією РОП служить аналіз ризиків, управління ризиками та кримінальний аналіз як інструмент встановлення взаємозв'язків між даними про злочинну діяльність та іншими даними, потенційно з ними пов'язаними, їх оцінювання та інтерпретацію, прогнозування розвитку досліджуваних подій.

Існує два шляхи встановлення гранично прийнятного ризику – декларативний та обґрунтований. У разі *декларативного* підходу значення прийнятного ризику встановлюється відповідно до нормативно-правових актів – законів, стандартів, правил, норм, якими визначені гранично допустимі (максимальні чи мінімальні) параметри певних чинників. Застосування РОП правоохоронним органом повинно здійснюватися в порядку, визначеному внутрівідомчими наказами. Правоохоронний орган зобов'язаний у своїй діяльності застосовувати РОП, враховуючи відповідні критерії ризику, зокрема, пов'язані з правопорушником, характером та видом протиправної дії, галузевими та секторальними особливостями системних кримінальних явищ, фінансовими втратами тощо. РОП має бути пропорційний характеру та масштабу діяльності правоохоронного органу. Наслідком не застосування РОП в системі протидії кримінальним загрозам є високі ризики зменшення надходжень до бюджету, проблеми з життєзабезпеченням населення та безробіттям тощо.

У разі *обґрунтованого* підходу значення прийнятного ризику визначається шляхом співставлення окремих видів ризику з рівнями «природного» ризику. Кінцеве значення оптимального гранично

прийнятного ризику встановлюється балансовими розрахунками між витратами, які необхідно нести на підтримання зазначеного рівня безпеки і величинами можливих збитків.

В наш час існують як математичні методи, так і методи обчислень для створення імовірнісних схем моделювання. Необхідне тільки наукове обґрунтування їхнього вибору і надійні експериментальні дані для того, щоб уводити відповідні параметри в ці моделі. РОП в діяльності правоохоронного органу є основою забезпечення національної, економічної та публічної безпеки, моніторингу процесів, що відбуваються у кримінальному середовищі та запобігання виникненню неконтрольованих криміногенних ситуацій.

Після оцінки ризику, правоохоронний орган повинен застосовувати свій РОП на постійній основі. Ефективність оцінки ризику повинна бути задокументована та відповідати положенням законодавства з питань забезпечення національної, економічної та публічної безпеки. Важливо, щоб детективи та аналітики, були навчені і дотримувалися правил, протоколів і процедур щодо аналізу та управління ризиками й протидії конкретним правопорушенням підслідних правоохоронному органу. Аналітики, які здійснюють ідентифікацію загроз, а також аналіз публічних процедур та послуг, фінансово-господарських операцій, а також аналізують ефективність реалізації заходів реагування на ризики надають рекомендації щодо коректності застосування заходів з мінімізації або усунення ризику та усунення вразливостей системи забезпечення національної, економічної та публічної безпеки.

Процедури правоохоронного органу повинні, як мінімум, містити вимоги щодо:

- *звітності;*
- *збору, структурування та зберігання даних;*
- *ризиковості особи (групи осіб)/об'єкта (підприємства, установи, організації)/події, явища;*
- *оцінки ризику;*
- *спеціальних заходів для високих ризиків.*

Політика та процедури правоохоронного органу також повинні:

- *пояснювати, алгоритм дій щодо виявлення підозрілих операцій (діяльності) та логіку застосування заходів реагування на ризики національної, економічної та публічної безпеки;*
- *визначати та пояснювати, який тип превентивного впливу (оперативні можливості, компетенції та юридичні інструменти окреслені повноваженнями суб'єктів контролю) застосовується для конкретних ситуацій (наприклад, ризиковості суб'єкта/ ризиковості управлінських рішень або послуг/ характеру ділових відносин, зв'язкам суб'єкта із низьким та високим ризиками);*
- *описувати усі процеси оперативного моніторингу окремих сфер життєдіяльності, зокрема економічної та/або бюджетної сфер: коли він проводиться (його частота), як він проводиться, як він переглядається.*
- *ресурсне забезпечення впровадження практики управління ризиками та оцінювання стану відповідних спроможностей правоохоронного органу як елементів стратегічного планування у сфері забезпечення національної, економічної та публічної безпеки;*
- *удосконалювати процедури кризового менеджменту, зокрема, впровадження універсальних алгоритмів узгоджених дій щодо реагування на кримінальні загрози національної, економічної та публічної безпеки на різних етапах їх розвитку;*
- *впроваджувати механізми забезпечення базових елементів і критеріїв оцінювання їх стійкості;*
- *забезпечувати впровадження спеціальних навчальних програм і курсів підвищення кваліфікації для працівників правоохоронного органу з питань забезпечення стійкості;*
- *сприяти набуттю працівниками правоохоронного органу необхідних знань і формування навичок щодо реагування на кримінальні загрози національної, економічної та публічної безпеки.*
- *визначати порядок формування та впровадження планів узгоджених дій з метою запобігання, реагування та подолання наслідків виникнення кримінальних загроз національної, економічної та публічної безпеки, щодо реагування на кримінальні загрози на різних етапах їх розвитку;*
- *визначати порядок, канали та формат обміну інформацією між правоохоронними органами про поточні та прогнозовані загрози, стан відповідних спроможностей, виявлені вразливості, а також план, механізми і процедури запобігання і реагування на них та відновлення у посткризовий період.*

Правоохоронному органу необхідно підтримувати в актуальному стані інформацію щодо системи державного регулювання, публічних процедур та послуг, фінансово-господарських відносин, що становлять високий ризик вчинення правопорушень, а також застосовувати спеціальні заходи для суб'єктів/ управлінських рішень та послуг/ділових відносин з високим ризиком. Важливо також пам'ятати, щодо управління та мінімізації ризиків необхідне залучення вищого керівництва правоохоронного органу та інших суб'єктів контролю. Вище керівництво, зрештою, відповідає за прийняття управлінських рішень, пов'язаних з процедурами та процесами, що мінімізують та контролюють ризики вчинення правопорушень.

Крок 4: розробка та вжиття заходів з мінімізації ризику.

Мінімізація ризиків полягає у реалізації управлінських рішень шляхом проведення заходів на основі РОП з нейтралізації загроз та усунення вразливостей систем національної, економічної та публічної безпеки. Джерелом загроз, що становлять високий ризик, виступають діяльність ОГ та ЗО, які задовольняють попит на кримінальні бізнес-моделі на ринку, фактори, що впливають на формування або посилення такого попиту, а також самі схеми та способи вчинення правопорушень, згенеровані кримінальні пропозиції для учасників ринку власниками ризику, зокрема «недобросовісними контролерами».

Коли відповідно до оцінки ризиків, проведеної правоохоронним органом буде визначено високий ризик: надання публічних послуг або прийняття управлінських рішень щодо розпорядження державними ресурсами; реєстраційних відомостей суб'єкта господарювання; фінансово-господарської діяльності; зв'язків необхідно розробити стратегії з мінімізації ризику (політики та процедури, призначені для зменшення високих ризиків) та застосувати їх до ситуацій із високим ризиком. Правоохоронний орган повинен напряму або опосередковано застосовувати засоби оперативного моніторингу і процедури, які дозволяють йому ефективно управляти ризиками, які були ним ідентифіковані. Він повинен слідкувати за ефективністю таких методів контролю, сприяти їх поліпшенню і покращувати їх. Засоби контролю і процедури повинні бути схвалені керівництвом правоохоронного органу, а заходи, вжиті для управління та мінімізації ризиків (незалежно від того, чи є вони високими або низькими), повинні відповідати стандартам системи національної стійкості.

До заходів і методів контролю можуть належати:

- *загальне навчання щодо існуючих способів вчинення злочинів підслідних правоохоронному органу та ризиків, які мають відношення до підтримання правопорядку, економічної або бюджетної сфер;*
- *цільове навчання для підвищення обізнаності правоохоронного органу або інших суб'єктів контролю щодо методів кримінального аналізу, аналізу ризиків, способів превентивного реагування на сили, явища та чинники, що мають більш високий ризик або проблеми, вади, недоліки системи, які породжують або посилюють схильність до порушення функціональності та/або піддатливість негативним впливам загроз національної, економічної та публічної безпеки, які також мають високий ризик, методик розслідування окремих видів злочинів на основі РОП;*
- *посилені або більш доцільні цільові заходи контролю або достатні оперативні можливості, компетенції та юридичні повноваження щодо перевірки суб'єктів / інцидентів з більш високим ризиком, які спрямовані на сприяння кращого розуміння про потенційне джерело ризику і отримання необхідної інформації для прийняття обґрунтованих управлінських рішень про дії (якщо публічні послуги, процедури, рішення/фінансово-господарські операції/ділові відносини можуть бути продовжені);*
- *періодичний огляд криміногенних процесів, бізнес-процесів, кримінальних циклів, послуг, дій контролюючих органів, за яких виникає ризик і періодична оцінка законодавства, інструментів можливого реагування на ризик правоохоронним органом та інших суб'єктів контролю, і власних процедур щодо превентивного впливу або кримінального переслідування з метою визначення зміни рівня ризику національної, економічної та публічної безпеки;*
- *періодичне здійснення перевірки відносин між представниками бізнесу та суб'єктами системи забезпечення національної, економічної та публічної безпеки, а також правоохоронним органом, задля визначення того, чи збільшився ризик національної, економічної та публічної безпеки.*

При присвоєнні *високого рівня ризику* правоохоронним органом застосовуються спеціальні заходи, які обираються в залежності від його інституціональних можливостей, а саме:

1. Превентивні заходи впливу (оголошення офіційного застереження про ризиковість операцій, постановка на оперативно-превентивний облік, перевірка фінансового та майнового стану (складання фінансового профілю), покладання судом обов'язків;
2. Застосовуватися спеціальних економічних та інших обмежувальних заходів (наприклад: види санкцій зазначені у ст.4 Закону України «Про санкції»);
3. Заходи оперативно-розшукового впливу з руйнування кримінальних бізнес-моделей та нейтралізації впливу ОГ та ЗО на зовнішнє середовище (шляхом проведення агентурних операцій (операцій під прикриттям), використовуючи конфіденційну допомогу громадян та інших оперативно-розшукових заходів обумовлених задумом превентивної тактики);
4. Зобов'язання інших суб'єктів контролю зреагувати на ризики, в межах їх повноважень (наприклад: Державна служба фінансового моніторингу України - виявлення та блокування фінансових операцій, Державна податкова служба України - блокування податкових накладних тощо), правоохоронних органів (притягнення до відповідальності за інше незначне правопорушення) тощо;
5. Кримінально-правовий вплив в межах досудового розслідування на осіб/групи, об'єкти, які є джерелом небезпеки для держави та суспільства (притягнення до кримінальної відповідальності правопорушника).

Для правопорушників або сфери злочинної діяльності з низьким рівнем ризику застосовуються спрощені заходи превентивного або адміністративно-правового впливу.

Крок 5: оцінка підходів та заходів з мінімізації ризику.

Частина оцінки ризику, яку здійснює правоохоронний орган, також повинна передбачати періодичний перегляд для перевірки ефективності існуючих протоколів та внутрішніх процедур, який включає:

- *політики та процедури правоохоронного органу;*
- *методики оцінки ризику щодо вчинення правопорушень у різних сферах;*
- *програму навчання (для працівників та вищого керівництва).*

Це означає, якщо на ринку пропонуються нові кримінальні послуги, виникають нові способи вчинення злочинів, до системи державного контролю долучаються інші суб'єкти контролю або змінюються їх повноваження, оцінку ризику слід оновити разом із процедурами щодо мінімізації ризиків. Перегляд або оцінка ризиків, пов'язаних з вчиненням правопорушень, має охоплювати всі компоненти, включаючи процедури щодо оцінки ризиків, мінімізації ризику та посиленого оперативного моніторингу. Це допоможе оцінити необхідність зміни наявних внутрішніх процедур або впровадження нових. Правоохоронний орган зобов'язаний здійснювати оцінку/переоцінку ризиків, у тому числі притаманних його діяльності, документувати їх результати, а також підтримувати в актуальному стані інформацію щодо оцінки ризиків, притаманних його діяльності (ризик-профіль правопорушника), ризику протиправної діяльності, ризик-рішень та ризик послуг таким чином, щоб бути здатним продемонструвати своє розуміння ризиків, що становлять загрозу життю та здоров'ю населення, втрат бюджету або зниження активності підприємницької діяльності тощо. Щодо ризикових суб'єктів, а також кримінальних подій та інцидентів з високим рівнем ризику правоохоронному органу потрібно буде вжити таких передбачених спеціальних заходів:

- *здійснювати переоцінку ризиків;*
- *підтримувати в актуальному стані інформацію щодо оцінки ризиковості суб'єктів.*

Що стосується критеріїв ризику вони повинні враховувати:

Наслідки (вплив загрози) заподіяння шкоди (збитків) охоронюваним законом цінностям (така оцінка проводиться на основі відомостей про ступінь тяжкості фактичного заподіяння шкоди, збитку в подібних випадках, потенційний масштаб поширення ймовірних негативних наслідків, що тягнуть за собою його заподіяння, з урахуванням складності подолання таких наслідків);

Ймовірність настання негативних подій, які можуть призвести до порушень прав і свобод громадян, втрат бюджету, зловживань, пов'язаних з отриманням та використанням міжнародної технічної допомоги, завдання шкоди (збитків) охоронюваним законом цінностям (враховуються попередні дані про фактичне заподіяння шкоди (збитків) внаслідок настання подій, викликаних певними загрозами та інцидентами, що характеризуються схожою або різною частотою випадків фактичного заподіяння шкоди (збитків);

Характеристика діяльності суб'єктів контролю сумлінність суб'єктів контролю (оцінюється з урахуванням відомостей про: реалізації суб'єктом контролю окреслених його компетенцією, юридичними повноваженнями та оперативними можливостями заходів щодо зниження ризику публічної безпеки, втрат бюджету, перешкоджанню зловживанням, пов'язаних з отриманням та використанням міжнародної технічної допомоги, заподіяння іншої шкоди й її запобігання; наявності впроваджених сертифікованих систем аналізу ризиків та кримінального аналізу, критеріїв оцінки ефективності роботи; надання суб'єктам контролю доступу до інформаційних ресурсів, достатніх в межах їх компетенції проводити аналіз ризиків; незалежну оцінку процедур кризового менеджменту, зокрема, впровадження універсальних алгоритмів узгоджених дій за результатами КЗОР; впровадження механізмів забезпечення і критеріїв оцінювання інституціональної стійкості базових елементів).

Концепція використання РОП у правоохоронній практиці є прогресивною, тому що вона є розвитком формули Ч. Беккаріа: «злочину краще запобігти, ніж потім карати за нього» [6, с. 222]. Цю формулу можна модернізувати так – для протидії, наприклад, економічній злочинності кризового типу потрібні реформи дозвільної системи, системи ліцензування, процедур входження та виходу з бізнесу, сфери державного нагляду та контролю, освіти та забезпечення доступу бізнесу до дешевих кредитів та ін., які б мали антикримінальний ефект, зокрема: 1) створювали умови для розвитку підприємництва. Забезпечували б здатність держави і суспільства своєчасно ідентифікувати загрози, виявляти вразливості та оцінювати ризики національної, економічної та публічної безпеки, запобігати або мінімізувати їх негативні впливи, ефективно реагувати та швидко і повномасштабно відновлюватися після реалізації загроз; 2) забезпечували б адекватне застосування засобів превентивного впливу та кримінально-правового захисту суспільних відносин, які охороняються спеціальними законами та/або законом про кримінальну відповідальність.

З огляду на зазначене, опис загроз та вразливостей, а також цілей, на вирішення яких необхідно спрямовувати зусилля правоохоронного органу та інших суб'єктів контролю для забезпечення на-

ціональної, економічної та публічної безпеки з метою нівелювання негативних наслідків прояву відповідних ризиків, можна викласти у такій послідовності:

1) аналіз зовнішніх та внутрішніх загроз і вразливостей для системи суспільних відносин, фінансово-економічної та суспільно-політичної сфери України;
2) аналіз інтенсивних (великих одноразових і непередбачуваних) та екстенсивних (менш масштабних, але регулярних) ризиків національної, економічної та публічної безпеки;
3) виявлення і типологізація ключових сфер криміналізації суспільних відносин, економіки (схеми, способи, інструменти, предмети та об'єкти посягання), а також механізмів та факторів, які обумовлюють формування кримінального попиту та кримінальної пропозиції на тіньовому ринку, джерел, що формують або генерують такий попит та пропозиції (ОЗУ, суб'єкти контролю, бізнес тощо);
4) інтеграція інформаційних потоків і систематизація статистичних зведень (комплексної адміністративної звітності) у сфері управління ризиками національної, економічної та публічної безпеки, з метою моніторингу внеску уповноваженого правоохоронного органу, інших суб'єктів контролю, а також регуляторних та інших правоохоронних органів, судової системи у дієвість та результативність функціонування системи національної, економічної та публічної безпеки;
5) аналіз секторальних ризиків національної, економічної та публічної безпеки та створення ефективних механізмів ризик-орієнтованого моніторингу потенційних джерел генерування кримінальних пропозицій на тіньовому ринку та факторів, що посилюють вразливість систем національної, економічної та публічної безпеки за результатами обробки правоохоронним органом зведених даних у розрізі окреслених компетенцій;
6) гармонізація регуляторної та антикорупційної державної політики шляхом відпрацювання ефективної ризик-орієнтованої системи виявлення та своєчасного реагування на джерело загрози, моніторингу ризик-рішень та ризик-послуг розпорядників бюджетних коштів та/або суб'єктів надання публічних послуг, а також тих фінансових операцій та/або протиправної діяльності, кінцевими вигодоодержувачами за якими є національні публічні діячі та/або пов'язані з ними чи близькі до них особи.

Мінімізація окреслених вище загальних загроз і вразливостей може стати вагомим підґрунтям підвищення дієвості, результативності та ефективності системи забезпечення національної, економічної та публічної безпеки, а також запорукою розробки, впровадження й подальшого поширення цілісного комплексу заходів аналітичного, оперативно-розшукового, кримінально-процесуального, кримінологічного характеру, який сприятиме переходу від традиційної протидії й боротьби з наслідками (симптомами) суспільно-небезпечних протиправних діянь до стратегії проактивного запобігання і системної нейтралізації факторів (причин) криміналізації суспільних відносин, національної економіки та сфери управління публічними фінансами.

УПРАВЛІННЯ АНАЛІЗОМ РИЗИКІВ

Запровадження ризик-орієнтованого підходу, з ключовою його складовою аналізом ризиків, у правоохоронну практику, для уможливлення превентивного впливу на процеси криміналізації суспільних відносин, з метою забезпечення національної, економічної та публічної безпеки, є більш ефективним способом захисту суспільства від шкоди, аніж кримінальні переслідування осіб причетних до протиправних дій після їх вчинення.

Діяльність уповноважених суб'єктів контролю відіграє важливу роль в системі захисту суспільства від процесів його криміналізації, зокрема шляхом:

(1) підвищення рівня поінформованості суб'єктів регулювання та їхнього розуміння ризиків національної, економічної та публічної безпеки; встановлення регулятивних зобов'язань та підтримки й сприяння сучасним практикам реагування на ризики;
(2) усунення загрози, забезпечення виконання та моніторингу дотримання обов'язків із забезпечення правопорядку, а також
(3) вжиття відповідних заходів у разі виявлення недоліків системи.

Правоохоронні органи повинні імплементувати ризик-орієнтований підхід, щоб виконувати ці функції ефективно та результативно. Широке впровадження цієї практики в діяльність усіх правоохоронних органів це прояв здатності держави вирішувати проблеми, що мають системний характер. Розглядати злочинність саме як кримінальну загрозу, а діяльність правоохоронних органів через призму спроможності державних інститутів щодо відвернення її проявів, допомагає сформувати принципово інші підходи до системи організації роботи правоохоронного сектору, зокрема в питаннях досудового розслідування та оперативно-розшукової діяльності.

Ризик-орієнтований підхід передбачає узгодження заходів уповноваженими суб'єктами контролю з реагування на ризики. Він надає суб'єктам контролю змогу розподіляти обмежені ресурси для мінімізації ризиків криміналізації суспільних відносин, що гармонізовано з національними пріоритетами. Формування правоохоронної діяльності, скерованої на ризики наприклад криміналіза-

ції бізнес процесів, освоювання бюджетних коштів та міжнародної технічної допомоги, зменшить шанси злочинців використовувати вади системи щоб вчинювати протиправні дії. Окрім того, цей підхід покращить якість інформації, до якої правоохоронні органи мають доступ. Це також надасть змогу уникати непотрібного навантаження на сферу надання публічних послуг, сектори економіки, учасників бізнес-процесів та види діяльності з низьким рівнем ризику під час виконання правоохоронної чи контрольної функції. Така умова надважлива для розвитку держави, суспільства, економіки, що зможе загалом знизити кримінальні ризики через транспарентність процесів у наданні публічних послуг та в економіці, також у забезпеченні правопорядку вцілому. Надійний ризик-орієнтований підхід охоплює належні стратегії для мінімізації усього спектра ризиків, як від сфер суспільних відносин, галузей економіки, видів діяльності та суб'єктів із підвищеним рівнем ризику, так і до сфер, галузей економіки, видів діяльності та суб'єктів із пониженим рівнем ризику. Ризик-орієнтований підхід, упроваджений у належний спосіб, забезпечить краще реагування, зменшить навантаження, а також надасть змогу скеровувати більшу кількість рішень щодо цього питання до компетенції тих осіб, які щонайкраще розуміються на їх прийнятті.

Взаємні оцінки продемонстрували, що перехід до ризик-орієнтованого підходу зумовлює появу чималих труднощів. Суб'єкти контролю повинні добре розуміти ризики, спиратися на надійну правову базу (стосовно зобов'язань та повноважень), відчувати політичну й організаційну підтримку, а також мати відповідні можливості, ресурси та компетентності, щоб забезпечувати успішне використання ризик-орієнтованого підходу у правоохоронній та регулятивній діяльності. Перехід від нормативно-орієнтованого підходу до ризик-орієнтованого займає певний час. На додачу до вироблення та впровадження комплексного набору інструментів для здійснення аналізу та оцінки ризиків необхідно також змінювати правоохоронну культуру та інвестувати в розвиток спроможностей та навчання працівників.

РОП слід використовувати спільно з (1) Методологією SOCTA (Оцінкою загроз організованої та серйозної злочинності). Для відома SOCTA є повним комплексним дослідженням організованої злочинності в ЄС, завдяки якому: визначаються реальні та потенційні чинники, фактори та загрози організованої злочинності, розробляються прогнози та можливі сценарії реагування з метою їх нівелювання та попередження; визначаються поточні та перспективні тенденції організованої злочинності, уточнюються особливості діяльності ключових злочинних угруповань і окремих злочинців на території країни та більш масштабно характеризуються фактори навколишнього середовища, які впливають на стан організованої злочинності в державі; відслідковується динаміка та взаємозв'язок між організованою злочинністю та прогресивними технологіями, які використовуються злочинцями; (2) методиками кримінального аналізу; (3) комплексом заходів з оцінювання ризиків та ін.

> ***Аналіз ризиків*** *- це сукупність процедур і методів обробки інформації щодо оцінки загроз національної, економічної та публічної безпеки, діяльності окремих осіб чи груп, підприємств, установ, організацій, причетними до злочинної діяльності, видів злочинів у певній сфері або їх наслідками, рівня негативного впливу на суспільство, підприємницьку діяльність, оцінки ступеню вразливості органів влади, зокрема судової системи, правоохоронних та контролюючих органів.*

Аналіз ризиків використовується на інституційному рівні, на трьох основних компонентах аналізу інформації, відповідно стратегічному, оперативному та тактичному. Цей тип аналітичного продукту має використовуватись в активній фазі діяльності правоохоронного органу в тому сенсі, що він орієнтує діяльність на виявлення, оцінювання та визначення ризиків вчинення кримінальних правопорушень, а також вжиття відповідних заходів щодо управління ризиками у спосіб та в обсязі, що забезпечують мінімізацію таких ризиків залежно від їх рівня, а також документування фактів протиправної діяльності до реєстрації інциденту / події / правопорушення на інституційному рівні. Це не виключає проведення аналізу ризиків у реактивному сегменті, у такому випадку, як правило, визначається поведінка, якої слід дотримуватись детективам у конкретних ситуаціях.

Аналіз ризиків як процес прийняття та реалізації управлінських рішень передбачає запобігання та мінімізацію кримінальних ризиків національної, економічної та публічної безпеки, припиненні, розкритті та розслідуванні злочинів підслідних правоохоронному органу, а також відверненні кримінальних загроз та удосконалення механізмів контролю з усунення недоліків системи, які породжують або посилюють схильність до порушення функціональності та/або піддатливість негативним впливам.

Система аналізу ризиків представлена трьома основними компонентами аналізу інформації: стратегічний; оперативний; тактичний.

У правоохоронному органі ризики повинні виділятися залежно від потреби визначення необхідного рівня точності або виходячи з наявного об'єму даних, а саме від трьох (*низький, середній, високий*) або п'яти (*дуже низький, помірний, допустимий, високий, катастрофічний*) рівнів ризику (щоб забезпечити замовнику вищу точність щодо рівня ризику).

Залежно від результатів проведення аналізу ризиків встановлюються рівні ризиків, зокрема для трирівневого підходу:

низький - за незначних рівнях загрози або коли рівень загрози переважає рівень уразливості, за незначного або помірного рівня впливу,

середній - за низького або помірного рівня впливу, коли рівень уразливості відповідає рівню загрози,

високий - за помірного або високого рівня впливу, коли рівень уразливості переважає рівень загрози.

СТРАТЕГІЧНИЙ РІВЕНЬ.

Аналіз ризику стратегічного рівня включає оцінку кримінального явища, діяльності організованих груп та злочинних організацій, криміногенної ситуації чи типу інцидентів, пов'язаних із зонами їх походження, часовими інтервалами та частотою, на середній та довгостроковій перспективі, на основі заздалегідь визначених критеріїв (показників).

Метою аналізу ризиків на стратегічному рівні, як першочергового кроку діяльності правоохоронного органу, повинно бути вивчення кримінального/криміногенного явища з метою оцінки його впливу на національної, економічної та публічної безпеки та управління ризиками з метою мінімізації ризиків та кращого забезпечення управління інституційними ресурсами. При цьому зосереджуються зусилля на господарських/виробничих, бюджетних, фіскальних процесах, інструментах вчинення злочинів, часових інтервалах (частоти застосування) та визначенні причинно-наслідкових зв'язків, втягуваності.

Аналіз ризиків стратегічного компоненту забезпечується на центральному рівні шляхом визначення ризиків, пов'язаних із кримінальними злочинами підслідними правоохоронному органу, криміногенними явищами чи деякими типами інцидентів, для обґрунтування управлінських рішень щодо певних напрямків та інструментів реагування. У такому випадку звіт щодо такого аналізу з визначенням прогнозованих наслідків охоплює проміжок часу, що перевищує один рік. Зазвичай сфери його поширення це національний або регіональний рівень (принаймні рівень області), при цьому обсяг аналізованих даних може встановити ризики на основі заздалегідь встановлених критеріїв.

Замовниками стратегічного аналізу ризиків можуть бути:

а) керівництво правоохоронного органу;
б) керівники територіальних управлінь правоохоронного органу;
в) центральні органи виконавчої влади чи інші державні, зокрема інші правоохоронні органи, в межах інституціональної компетенції із забезпечення національної, економічної та публічної безпеки, а також профільні комітети Верховної Ради України.

Користувачами аналізу ризику стратегічного рівня можуть бути:

- *керівники середньої ланки правоохоронного органу або окремі працівники відповідно до функціональних обов'язків;*
- *установи, організації з якими правоохоронним органом підписані відповідні угоди;*
- *інші установи, організації відповідно до їх запиту у разі згоди на це керівництва правоохоронного органу.*

У разі, якщо звіт містить відомості з обмеженим доступом, керівництвом правоохоронного органу на свій розсуд можуть бути прийняте одне із наступних рішень:

- *направити звіт замовнику (користувачу) відповідно до правил секретного діловодства;*
- *відмовити у наданні матеріалів звіту;*
- *надати усічений звіт.*

Звіт про аналіз ризиків готується уповноваженими аналітиками відповідно до посадових обов'язків або на підставі запиту/розпорядження керівника, який вказує на явище, часовий проміжок, а також інші показники, що становлять інтерес для аналізу.

ОПЕРАТИВНИЙ РІВЕНЬ.

Аналіз ризику оперативного рівня представляється як продукт, який готується аналітиком, відповідно до запиту уповноваженої особи щодо ризиків вчинення певного виду злочинів у різних сферах суспільних відносин та галузях економіки, або пов'язаних з розпорядженням бюджетними коштами, а також з отриманням та використанням міжнародної технічної допомоги. Він може складатися у разі прийняття рішень щодо: превентивного оперативно-розшукового втручання в процеси, що відбуваються у кримінальному середовищі; руйнування кримінальної інфраструктури; розслідування кримінальних проваджень; нейтралізації впливу організованих груп та злочинних організацій тощо. Замовниками та користувачами такого аналізу можуть бути детективи правоохоронного органу, незалежно від їх рівня.

Звіт за результатами аналізу ризиків є аналітичною підтримкою роботи детективів та переслідує мету виявлення потенційних ризиків, про які раніше не було відомо, але які становлять ризик вчинення злочинів або створюють підґрунтя для останнього.

Цілі звіту за результатами аналізу ризиків щодо превентивного втручання у криміногенні процеси, визначаються на основі показників ризику, попередньо встановлених аналітиком, залежно від кримінального злочину, що розглядається.

Для ідентифікації окремих джерел ризику вчинення злочинів або обґрунтованої підозри щодо цього, використовуються всі бази даних, зокрема автоматизована система аналізу та управління ризиками, а також відкриті джерела. За необхідності, за результатами аналізу ризиків, цей великий обсяг даних відображається у змісті звіту у структурованій, пояснювальній формі на основі виявлених або заздалегідь визначених показників ризику.

Виявлені ризики, висновки та рекомендації, що знайшли відображення у змісті звіту про результати аналізу ризиків, надаються детективам кримінальної розвідки для оцінки можливості превентивного втручання у криміногенні процеси. Матеріали, що мають достатню кількість даних, інформації, версій, гіпотез та висновків та підтверджуються результатами проведених спеціальних операцій, зокрема із застосуванням оперативно-технічних заходів, а також контрольно-перевірочною діяльністю, з метою одержання доказової бази, можуть бути підставою для відкриття кримінального провадження.

ТАКТИЧНИЙ РІВЕНЬ.

Аналіз ризику тактичного рівня включає оцінку видів злочинів або серії інцидентів у районах їх виникнення, за часовими інтервалами та частотою, за короткий та середньостроковий проміжок часу (до одного року), відповідно до сфери аналізу ризиків та рівню латентності злочинів.

Аналіз ризику тактичного рівня може бути складений на місцевому рівні для обмежених територій, наприклад, на рівні населеного пункту, області або регіону, залежно від компетенції територіальних підрозділів правоохоронного органу, шляхом аналізу інформації, даних та відомостей, доступних протягом 24-годин. У такому разі типи звіту розрізняють РТ24 (24-годинний тактичний ризик), РТ30 (30-денний тактичний ризик) та за запитом в ТАРЗ (тактичний аналіз ризиків за запитом).

Звіти про результати аналізу ризиків тактичного рівня можуть готуватися на вимогу керівників територіальних управлінь правоохоронного органу в регіоні, області, місті або за запитом уповноваженої особи та лише типу РТ24 та РТ30.

Аналіз ризиків тактичного рівня є способом виявлення латентних злочинів, віднесених до компетенції правоохоронного органу, тобто тих, які не стали предметом реагування з боку останнього, шляхом моніторингу інших, пов'язаних з ними правопорушень, інцидентів.

Тип звіту обирається залежно від наявних даних або часового інтервалу, що підлягає аналізу.

Звіти про результати аналізу ризиків тактичного рівня надаються замовнику/користувачу для забезпечення об'єктивного уявлення про реальний стан злочинності.

Етапи виконання аналізу ризиків:

1. Визначення мети та кола завдань, які потребують вирішення. Передбачає: визначення виконавця та оформлення запиту на проведення аналізу, при цьому орієнтовний план визначає вид необхідних даних, їхнє джерело, аналітичні техніки, методи аналізу, термін реалізації та форми розповсюдження.

2. Визначення об'єкту аналізу (особи, групи, явища) та теми аналізу. Передбачає: збирання даних та інформації, дії відповідно до плану.

3. Оцінка інформації. Передбачає: оцінку надійності джерел інформації та її достовірності, що робить подальшу інтерпретацію інформації більш обґрунтованою.

4. Впорядкування. Передбачає: відсіювання неправдивих, несуттєвих даних, впорядкування решти інформації з метою встановлення взаємозв'язків між її складовими.

5. Аналіз. Передбачає: ґрунтовну інтерпретацію інформації; опрацювання максимально точних висновків та прогнозів, трендів і закономірностей; надання рекомендацій; інформування про факти щодо діяльності окремих ОГ та ЗО, їхній потенціал та слабкі сторони.

6. Представлення результатів. Передбачає: підсумовування результатів процесу накопичення та аналізу інформації, а також представлення результатів оперативного процесу; визначення виразних зв'язків між фактами та оцінками, висновками та прогнозами; часто вимагає додаткового навчання у сфері написання текстів або використання програмного забезпечення для візуалізації матеріалу.

7. Розповсюдження. Передбачає: постачання звіту зовнішнім та внутрішнім замовникам/користувачам та, у разі потреби, особам, які надали дані та інформацію у якості допомоги та власного внеску в побудову якісної системи національної, економічної та публічної безпеки.

8. Оцінювання результатів (здійснюється після завершення аналізу). Передбачає дві форми: одна спрямовується на вивчення рівня виконаної роботи аналітичним підрозділом (аналітиками), а також з'ясування, що саме вплинуло на якість їхньої роботи (знання, досвід); друга концентрується на результативності, тобто оцінці, чи був продукт аналізу корисним у роботі замовника, який рівень підтримки він забезпечив та чи був він, на думку замовника, достовірним і своєчасним.

Вимоги, що висуваються до кожного етапу проведення аналізу ризиків:

1. Визначення мети, кола завдань та теми аналізу може бути встановлена як на прохання замовника, так і аналітиком самостійно відповідно до функціональних обов'язків. Якщо це відбувається за бажанням замовника, запит повинен бути сформульований ним письмово у довільній формі за формою визначеною відомчим нормативним актом, як це передбачено в угоді про співпрацю.

На цьому етапі аналітик повинен враховувати наступні критерії:

а) тема та мета повинні бути чітко визначені;
б) забезпечити доступ до даних та інформації, що є предметом аналізу;
в) вимоги клієнта не перевищуватиме матеріально-технічні та інші ресурсні можливості;
г) розумні умови, залежно від наявних даних та інформації;

Технічне завдання щодо проведення аналізу ризиків стратегічного, тактичного та операційного рівнів, що окреслене у цій методології, повинне співвідноситись з іншими затвердженими методиками або процедурами аналізу інформації, а також наказами та положеннями, що врегульовують питання збору інформації.

У разі виникнення обставин, зазначених у нормативних документах як таких що унеможливлюють проведення аналізу ризиків, аналітик має право відмовити замовнику в проведенні аналізу ризиків про що письмово доповідає керівникові, який доручив останньому проведення такого аналізу, про що також інформується замовник.

2. Збір інформації з метою проведення аналізу ризиків здійснюється з усіх доступних джерел (закритих та відкритих).

Збір інформації для аналізу ризиків повинен виконуватись відповідно до існуючих процедур / методик для кожного компоненту аналізу інформації.

3. Оцінка інформації. На цьому етапі аналітик використовуватиме наступні методики:

а) Фільтрування інформації - відмова від інформації, яка не є релевантною, щоб зосередитись на важливому;
б) Категоризація інформації - це відбір / класифікація даних за категоріями та логічними критеріями;
в) Пріоритетність - сортування зібраної інформації та упорядкування її за важливістю та актуальністю;
г) Оцінка інформації - це процес перевірки надійності джерела та достовірності інформації, отриманої з різних джерел;
д) Агрегація інформації - передбачає підрахунок даних, їх комбінування та обчислення середнього показника, зосередження уваги на найважливішому;
е) Порівняння - це зіставлення окремих елементів / інцидентів, щоб з'ясувати наявність чи відсутність взаємозв'язку між ними;
є) Кореляція - статистичний прийом, який допомагає встановити взаємозв'язок між одним набором даних та іншим;
ж) Причинність та пояснення - продовжує техніку кореляції, яка визначає причинно-наслідковий зв'язок між окремими факторами.

Аналіз та інтерпретація дозволять виявити існуючі умови, які впливають на досліджувану проблему та отримання відповіді на поставлені питання. Він описує та аналізує контекст, в якому знаходиться проблема, та забезпечує основу для порівняння джерел загрози та рівнів їх наслідків, одночасно надаючи можливість виявити інформаційні прогалини.

Аналіз ризиків та їх інтерпретація для кожного компонента (стратегічного, оперативного та тактичного) проводитимуться у відповідності з діючими методологіями, методиками чи процедурами.

Ідентифікація ризику проводиться на етапі його аналізу, враховуючи результати кримінального аналізу, шляхом виділення генеруючих елементів ризику та загрози.

Методи ідентифікації ризиків:

Карта перевірки (чек-лист) - використання певного сформованого переліку питань, для перевірки стану виконання процесу;

Аналіз блок-схем - послідовний аналіз виконуваного процесу, послідовність виконання якого відображено у графічний спосіб;

Порівняння з еталонними критеріями (бенчмаркінг) - систематичний пошук і впровадження найкращих практик роботи правоохоронних органів або структурно-функціональної та правозастосовної моделі протидії економічним злочинам для порівняння із власною системою організації роботи та переймання найбільш вдалих методів роботи;

Сценарне планування дослідження зовнішнього середовища, що впливає на діяльність правоохоронного органу, стосовно наявності визначених елементів (predetermined elements) і ключових невизначеностей (key uncertainties) та їх комбінування для формулювання альтернативних сценаріїв майбутнього.

Кожен із зазначених методів можна використовувати на практиці, що допоможе керівництву правоохоронного органу ідентифікувати ризики, зокрема під час: опитувань; мозкових штурмів; засідань робочих груп (з управління ризиками) / робочих (оперативних) нарад.

В залежності від конкретної ситуації, виявлення ризику здійснюється шляхом аналізу загальних або конкретних заздалегідь визначених показників об'єкту, що підлягає аналізу.

Показники ризику визначаються шляхом аналізу даних із офіційних джерел (власні бази даних правоохоронного органу або тих, до яких останній має доступ, статистичні матеріали тощо), які підтверджені іншими даними з відкритих джерел.

Далі ризик повинен оцінюватися на основі деяких загальних показників:
- еволюція загальної кількості інцидентів, що підлягають аналізу, зафіксованих за певний проміжок часу, порівняно з аналогічними періодами попередніх років;
- динаміка спричинених збитків, втрат бюджету (податкових надходжень та/або освоювання бюджетних коштів), кількості жертв / інцидентів за аналізований період;
- сфери, географічне розташування, місце виникнення інцидентів та / або жертв, секторів та місць втрат бюджету;
- середнє значення інцидентів та / або жертв, сум втрат бюджету у визначений проміжок, а також за сферою та місцем виникнення;
- часові інтервали, в яких відбуваються інциденти;
- існування та вплив зовнішніх економічних, соціальних та географічних факторів;
- встановлення взаємозв'язку між інцидентами, що аналізуються, та діями осіб (фізичних, юридичних), які знаходяться на оперативному обліку або відносно яких є інформація про причетність до протиправної діяльності.

Під час аналізу, на стадії саме оцінки загрози, аналітик повинен визначити, що саме спричиняє загрозу, в якій формі вона може бути реалізована, у разі якщо буде втілена, які наслідки матиме для держави, суспільства, економіки, бюджету, на які сфери суспільних відносин, сектори економіки або роботи державних органів вплине. При оцінці загрози може бути зроблений висновок про її відсутність або зменшення її рівня. Такий висновок є також важливим, його треба розглядати рівнозначним, як і у випадках оцінки загрози з високим рівнем впливу.

Аналітик під час аналізу ризиків повинен враховувати наступне:
- що загроза, як сила, яка має намір та можливості заподіяти шкоду, не вважається ризиком, якщо у нас відсутні вразливості, тобто слабкі місця системи, які може використати потенційний правопорушник;
- загроза завжди повинна сприйматися як ймовірнісна категорія, тому у разі її реалізації вона вже виступатиме як ситуація або стан речей;
- у зв'язку з тим, що рисою, яка притаманна загрозі є негативний вплив (шкідливі наслідки), у разі його відсутності, треба говорити не про загрозу, а швидше за все про фактор впливу.

Під час ідентифікації, опису та оцінки загрози необхідно враховувати дві загальні характеристики, що її визначають це ймовірність та вплив.

Рівень загрози розраховується на основі матриць 3×3 або 5×5, при цьому імпліцитно (неявний, прихований, такий, що (на відміну від експліцитного) може бути виявлений тільки через свої зв'язки з іншими об'єктами чи процесами) присвоюється значення як для впливу, так і для ймовірності за шкалою від 1 до 3 (ймовірність/вплив):

1 - низька/низький;
2 - середня/помірний;
3 - висока/високий;

або шкалою від 1 до 5 (ймовірність/вплив):

1 - дуже низька/дуже низький;
2 - низька/помірний;
3 - помірна/допустимий;
4 - висока/високий;
5 - дуже висока / катастрофічний.

Результат, отриманий на перетині між двома осями, представляє рівень загрози (у матриці 3×3 максимальний рівень досягає значення 9, а в типі 5×5 максимальне значення становить 25, тобто значення рівня загрози обчислюється шляхом множення значень ймовірності та впливу).

Залежно від отриманого результату, аналітик встановлює такі рівні загрози:

1-3	низька загроза	1	дуже низький рівень загрози
3-6	середня загроза	2, 3	помірний рівень загрози
6-9	висока загроза	4, 5, 6	допустимий рівень загрози
		8, 9, 10, 12	високий рівень загрози
		15, 16, 20, 25	катастрофічний рівень загрози

Для кращого графічного відображення рівнів загрози / ризику рекомендується включати кольорову схему до змісту звіту про результати аналізу.

Якісна оцінка рівня загрози

	ІМОВІРНІСТЬ	ВПЛИВ
	ОПИС	
низька / низький	➢ Виходячи з аналізу попередніх періодів, спостерігається стійка позитивна динаміка на зменшення випадків/масштабів негативних явищ, ресурсів на їх реалізацію, не відбувається інтелектуалізація протиправної діяльності, незмінність способів досягнення кримінальних цілей; ➢ Існують несприятливі внутрішні та зовнішні фактори для реалізації загрози; ➢ П/о володіє інформацією (А1, В2) з інших закритих та відкритих джерел, яка підтверджує протилежне.	➢ Наслідки: буде завдана незначна шкода або, як правило, не буде заподіяно шкоди національній, економічній та публічній безпеці (регіональній безпеці), а також системі функціонування державних інституцій, веденню господарської діяльності та соціальній сфері; ➢ Вони впливатимуть на невеликі території / сектори економіки /явища і жодним чином не впливатимуть на сфери життєдіяльності/економіку.
середня / помірний	➢ Присутня динаміка коливань щодо кількості/масштабів розповсюдження негативних явищ, задіяння ресурсів на їх реалізацію, кількості суб'єктів кримінальних пропозицій у попередні періоди, відбувається незначна інтелектуалізація протиправної діяльності, частково змінюються способи досягнення кримінальних цілей; ➢ Відсутність відповідних внутрішніх та зовнішніх каталітичних факторів; ➢ Часткове підтвердження або відсутність інформації.	➢ Наслідки: буде завдана помірна шкода національній, економічній та публічній безпеці (регіональній безпеці), та соціальній сфері; ➢ Вона впливатимуть на конкретні обмежені території / сфери (наприклад, на регіональному, місцевому рівні, певних галузях, секторах економіки), окремі напрями освоєння бюджетних коштів, а також міжнародної технічної допомоги або на частини деяких областей / явищ
висока/ високий	➢ Виходячи з аналізу попередніх періодів, спостерігається динаміка на збільшення кількості/масштабів розповсюдження негативних явищ, ресурсів на їх реалізацію, кількості суб'єктів кримінальних пропозицій, відбувається значна інтелектуалізація протиправної діяльності, суттєво змінюються способи досягнення кримінальних цілей; ➢ Існують внутрішні та зовнішні каталітичні фактори; ➢ Достовірність інформації підтверджується з інших закритих та відкритих джерел	➢ Наслідки: буде заподіяно значної шкоди національній, економічній та публічній безпеці (регіональній безпеці), а також соціальній сфері; ➢ Вони впливатимуть на значні території (наприклад, на національному або регіональному рівні) або на області вцілому / явища

Оцінка вразливості передбачає оцінку здатності системи реагувати на загрозу. У цьому сенсі аналітик враховуватиме такі компоненти:

1. оперативні можливості та компетентність працівників;
2. компетенцію та юридичні повноваження органу.

Рівень вразливості	Оперативні можливості та компетентності працівників	Компетенції та юридичні повноваження
Високий	Недостатньо технічних, людських та інституційних ресурсів	Відсутні повноваження, компетенції та інструменти впливу (правові, методичні) або відсутність можливості реагувати на загрози
Середній	Помірні технічні, людські (кількість, знання, уміння та навички) та інституційні ресурси	Помірний об'єм юридичних повноважень та / або компетенцій, що дозволяють певною мірою реагувати на загрози
Низький	Достатньо технічних, людських та інституційних ресурсів	Достатній рівень компетенцій та об'єм юридичних повноважень для реагування на загрозу

Послідовність оцінки ризику:

1) виявлення джерел і причин ризику, етапів і характеру дій, при проходженні та виконанні яких виникає ризик;
2) ідентифікація всіх можливих ризиків, властивих даній галузі, сфері економіки, розподілу бюджетних коштів;
3) оцінка рівня окремих секторальних ризиків і ризиків в цілому у різних сферах життєдіяльності, а також бюджетній, податковій, митній, грошово-кредитній та інвестиційній сферах, що визначає механізми та інструменти їх мінімізації;
4) визначення допустимого рівня ризику;
5) розробка заходів щодо зниження ризику, виходячи з інституціональної спроможності.

Оцінка ризику:

- має на меті виявити та дослідити вразливі сфери національної, економічної та публічної безпек вцілому, а також вразливі місця до кримінальних загроз бюджетної, податкової, митної, грошово-кредитної та інвестиційної сфер, які використовуються або якими можуть скористатися, щоб надати рекомендації із зазначенням інструментів та механізмів їх усунення;
- при цьому враховується не тільки характер вразливого сектору, але й характер потенційних джерел (суб'єктів) загрози (наприклад ОГ та ЗО, корумпованих можновладців тощо), та рівень складності режиму їх роботи;
- комбінація з поєднання передбачуваного рівня ймовірності та передбачуваного рівня впливу загрози є ризиком, на основі якого складається профіль ризику;

Оцінка ризику проводиться за трирівневою шкалою, а саме:

1. Оцінка ймовірності матеріалізації виявленого ризику полягає у визначенні вірогідності настання конкретного результату і здійснюється шляхом:

а) спостереження за матеріалізацією подібних ризиків у минулому;
б) аналізу обставин (причин), які сприяли/сприяють виникненню ризиків;
в) використання шкал для оцінки ймовірності матеріалізації ризику, відповідно трьох або п'яти рівнів ймовірності, як зазначено у таблицях нижче:

	Рівень ймовірності	Пояснення
1.	**Низька (0% - 19%) (можливо)**	навряд чи це станеться у довгостроковій перспективі; цього ще не траплялося.
2.	**Середня (20% - 79%) (Ймовірно)**	ймовірно, це станеться у середньостроковій перспективі; це траплялося періодично кілька разів за останній рік / роки.
3.	**Висока (80% - 100%) (Майже впевнений)**	дуже ймовірно, що це станеться найближчим часом; це траплялося системно багато разів за останній рік.

2. Оцінка впливу на економічну безпеку (об'єкт) у випадку матеріалізації ризиків являє собою наслідки для об'єкту впливу, які можуть бути, залежно від характеру ризику, негативними чи позитивними і проводяться згідно з таблицею:

	Рівень впливу / наслідки	Пояснення
1.	низький	З дуже низьким впливом на сфери або діяльність структури та досягнення цілей.
2.	середній	З середнім впливом на сфери або діяльність структури та досягнення цілей.
3.	високий	Зі значним впливом на сфери або діяльність структури та досягнення цілей.

3. Оцінка впливу ризику - це наслідки, поєднання ймовірності та впливу, які може відчувати система національної, економічної та публічної безпеки (об'єкт впливу) у випадку матеріалізації ризику. Рівень ризику обчислюється на основі матриці 3x3 або 5x5, представленої вище, у разі чого кожному типу аналізованого факту надається оцінка, як для впливу, так і для ймовірності за шкалами від 1 до 3 або від 1 до 5, наступним чином:

а) через матрицю 3×3: 1 - низький, 2 - середній, 3 - високий;

б) через матрицю 5×5: 1 - низький; 2 - помірний, 3 - допустимий, 4 - високий і 5 - катастрофічний.

Оцінка впливу ризику визначається наступним чином:

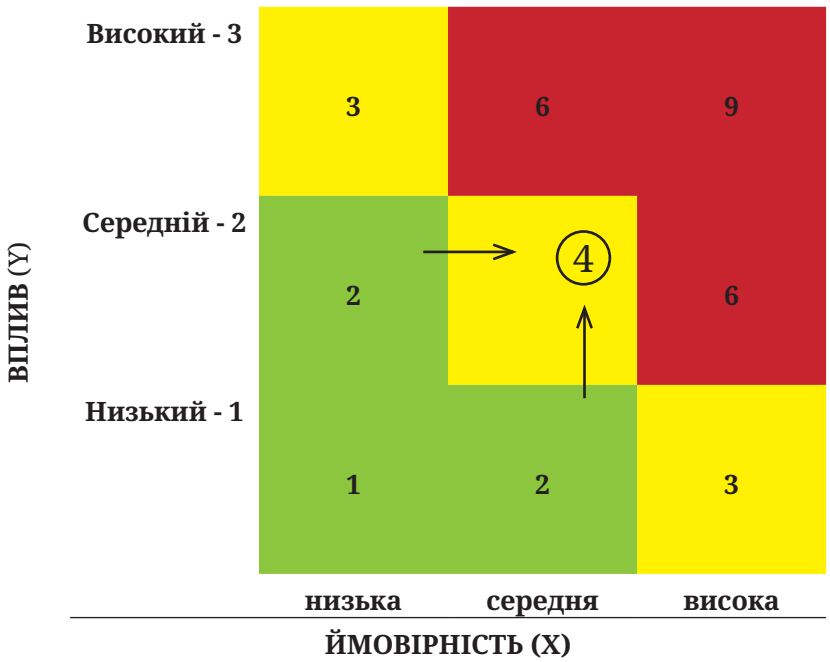
ймовірність × вплив (X × Y)

а) Шкала оцінки ризику за допомогою матриці "3×3" представлена графічно наступним чином:



ПРИМІТКА: Рядки матриці описують варіацію ймовірності, а стовпці - варіацію впливу. Схильність до ризику відбувається при перетині рядків із стовпцями.

Приклад вирішення матриці оцінки ризику типу 3×3.



Якщо ми реєструємо значення удару 2, а значення ймовірності 2, результат оцінки ризику дорівнює 4, що означає, що ми маємо середній рівень ризику (жовтий колір).

Залежно від отриманого результату, аналітик у звіті визначить такі рівні ризику (за п'ятирівневою відповідно):

1-3	низький ризик
3-4	середній ризик
6-9	високий ризик

1	Низький ризик
2, 3	помірний ризик
4, 5, 6	допустимий ризик
8, 9, 10, 12	високий ризик
15, 16, 20, 25	катастрофічний ризик

Встановлення відповідності й співвідношення між оцінкою загрози та оцінкою ризику і є метою оцінки. На першій фазі ціллю є загроза, а на другій фазі увага зосереджується на сфері життєдіяльності або об'єкті можливого впливу, які/який є вразлив(і)-им і може стати ціллю загрози. Сфера життєдіяльності (об'єкт впливу) може бути вразливим, навіть якщо відсутні загрози.

Якщо неможливо визначити ризики кількісно або їм не можуть бути присвоєні певні значення, вони оцінюються відповідно до: кількості попереджень; частоти, масштабів (географії) прояву; сум збитків та кількості вразливостей або у співвідношенні з іншими факторами ризику. Вони також класифікуються за 3 або 5 рівневою шкалою ризику, залежно від наявних даних та інформації.

УПРАВЛІННЯ РИЗИКАМИ

Природа ризику така, що, якщо його не обмежувати і не проводити превентивні заходи, він подібно газу може заповнити собою весь вільний від перешкод простір. Тоді вірогідність реалізації ризиків і об'єм їхнього кумулятивного негативного економічного (фінансового) ефекту з часом зростатиме.

За допомогою сучасних методів AI (штучного інтелекту) та ML (машинного навчання), а також сил, засобів і методів кримінальної розвідки (- далі КР) можна з достатньою повнотою простежити, як виникає злочинний задум, у яких конкретних діяннях він реалізується на різних етапах підготовки та скоєння злочинів, які фактори зумовили його виникнення в конкретних умовах місця та часу, які простежуються тенденції та прояви злочинності, сфери її найінтенсивнішого поширення тощо.

Базова модель управління ризиками національної, економічної та публічної безпеки правоохоронного органу включає трирівневу систему реагування на ризики та фактори, що їх обумовлюють:

Перший рівень, належить детективам, що проводять досудове розслідування, уповноваженим особам, які застосовують заходи превентивного впливу та проводять аналітичні дослідження, тобто організаторам будь-яких процедур та процесів в правоохоронному органі - керівникам середньої ланки, детективам та аналітикам, які стикаються з факторами ризику щодня і мають всіляко попереджати поточні інциденти, а у разі потреби інформувати про виникнення загроз або виявлення інциденту керівництво правоохоронного органу або інших суб'єктів контролю.

Другий рівень, належить спеціально уповноваженим підрозділам внутрішнього контролю (власної безпеки), кібербезпеки правоохоронного органу, а також аналітиками, які спеціалізуються на проведенні аналізу ризиків в їхніх різних варіантах і формах. Сюди належать усі підрозділи, основною сферою діяльності яких є процедури внутрішнього контролю. І які спільно з керівниками середньої ланки, детективами/аналітиками беруть участь в розробці та подальшому впровадженні в практику методик кримінального аналізу, аналізу ризиків та розслідування злочинів, схем, регламентів і внутрішніх нормативів як виключно організаційно-розпорядчого, так і операційно-технічного характеру. Цей рівень починає формуватися при переході від стадії повторюваності до стадії регламентованості й формує ланцюг зворотного зв'язку, з якого керівники правоохоронного органу та інших суб'єктів контролю починають отримувати перші відомості про неочевидні для них ризики, а також інциденти в системі забезпечення національної, економічної та публічної безпеки в цілому та про інституціональні уразливості суб'єктів контролю зокрема. На такому етапі керівництву правоохоронного органу необхідно усвідомлювати дві базові істини: кожен впроваджуваний регламент не є остаточним, його варто періодично переглядати на предмет відповідності вимогам сьогодення; належною реакцією на кожен новий виявлений ризик є оцінка його можливих наслідків. І тільки після цього (при необхідності) — розробка заходів з його усунення і мінімізації.

Третій рівень передбачає застосування групи внутрішнього аудиту (ГВА), яка може складатися з власних постійних співробітників або залучених зовні фахівців, представників Ради громадського контролю та ін., ключовою характеристикою яких є незалежність в оцінці процесів і систем правоохоронного органу, а основне завдання — оцінка адекватності й ефективності системи внутрішнього контролю й управління ризиками. Внутрішній аудит — це незалежна діяльність з перевірки і оцінки роботи правоохоронного органу в його ж інтересах. Внутрішній аудит допомагає правоохоронно-

му органу досягти поставлених цілей, використовуючи систематизований і послідовний підхід до оцінки і підвищення ефективності процесів управління ризиками, контролю і корпоративного управління. У діяльність ГВА, що, як правило, здійснюється на плановій основі, входить оцінка стану внутрішнього середовища правоохоронного органу, методик розслідування окремих видів злочинів, адекватності застосування та ефективності превентивних заходів впливу, наявність сертифікації у використовуваних аналітичних платформ для кримінального аналізу та аналізу ризиків, відповідність існуючих внутрішніх процедур ILP-моделі правоохоронного органу, й впроваджених в них засобів внутрішнього контролю, окремих фактів і аспектів оцінки ефективності роботи органу, систем управління ризиками. Одним з ключових завдань ГВА є оцінка корупційних ризиків, оскільки виключна монополія на боротьбу з окремими видами злочину породжує формування різних форм підкупу з боку учасників кримінального середовища, тіньового ринку. Репутаційний ризик від функціонування корупційних схем можна порівняти з наслідками реалізації критичного ризику, він здатний значно похитнути легітимність правоохоронного органу та довіру до нього з боку суспільства, бізнесу, донорів та інших зарубіжних правоохоронних інституцій.

Виходячи з інституціональних можливостей правоохоронного органу одним із інструментів мінімізації ризиків є застосування глибоких, спеціальних, тривалих (в ідеалі постійних) агентурних операцій, а саме виконання спеціального завдання, агентурне спостереження (стратегічні агентурні операції) та контроль за вчиненням злочину, зокрема контрольоване постачання. Але це зовсім не означає, що інші заходи кримінальної розвідки не мають жодного потенціалу до системи управління ризиками.

По-перше, навіть при проведенні разового заходу можна отримати інформацію, по заздалегідь визначеному профілю ризиків, для проведення аналізу ризиків або кримінального аналізу.

По-друге, під час проведення суто заходів кримінальної розвідки працівники правоохоронного органу отримують значний обсяг так званої попутної інформації. Причому далеко не вся інформація виявляється оперативним шляхом, оскільки на її отримання порівняно рідко орієнтувалися оперативні джерела інформації. Тим часом, можливості оперативних джерел інформації, зокрема детективів, які працюють під прикриттям у зборі такої інформації досить значні.

По-третє, сконцентрована, систематизована та збагачена оперативна інформація, яка отримана та внесена до баз правоохоронного органу для аналітичного дослідження, за результатами проведення всіх заходів КР (незалежно від їх поділу за ступенем значимості), є якісно іншим змістом (порівняно з розрізненими даними) і при грамотному використанні штучного інтелекту може стати незамінним джерелом емпіричних даних, необхідних для цілей кримінального аналізу (аналізу ризиків).

КР, що скеровується аналітикою сама є джерелом інформації для кримінального аналізу та аналізу ризиків. Для вивчення злочинності та протидії її проявам виникає потреба в оцінюванні способів впливу різних загроз на систему суспільних відносин, наприклад:

SOCTA - Методологія «Оцінка загрози з боку особливо небезпечних форм організованої злочинності», є продуктом системного аналізу інформації правоохоронців про кримінальну діяльність і групи, що становлять загрозу для ЄС, щоб допомогти керівникам у визначенні пріоритетів серед загроз організованої злочинності;

IOCTA - “Оцінка загроз від організованої злочинності в Інтернеті”, є усталеною практикою країн-членів ЄС та залишається важливим інструментом управління та ухвалення політичних рішень, що використовуються фахівцями з протидії кіберзлочинності, у тому числі й транснаціональній, для розробки державних програм на стратегічному рівні, визначення пріоритетів та розподілу ресурсів на операційному рівні;

TE-SAT щорічний звіт Європолу про ситуацію з тероризмом і тенденції в ЄС, містить огляд явища тероризму в ЄС за певний рік. Він пропонує співробітникам правоохоронних органів, політикам і широкій громадськості факти та цифри про тероризм в ЄС, а також визначає тенденції розвитку злочинності терористичного спрямування, на основі інформації, яку країни-члени надають Європолу.

Відповідно до діючого законодавства переважна кількість завдань правоохоронних органів, пов’язана з реалізацією превентивної функції у забезпеченні національної, економічної та публічної безпеки. Суттєвою ознакою поняття «превенція» є наявність певної низки дій чи подій (правопорушення, інциденти), одні з яких передують іншим і випереджають очікувані наслідки від попередніх. Мова йде про випередження в чому-небудь, дій чи подій котрі передують настанню певних подій чи явищ. На відміну від попередження, запобігання та припинення результат превенції є кращим, оскільки він не обтяжений наслідками дій і не потребує інших заходів. Поняття «превенція» в аспекті кримінальної розвідки та в контексті забезпечення національної, економічної та публічної безпеки, а також використання її за логікою РОП, розглядається як врегульований нормами оперативно-роз-

шукового та кримінального процесуального законодавства випереджувальний вплив на джерела загроз та фактори, що сприяють криміналізації суспільних відносин.

> *Чому саме ми говоримо про поєднання ризик-орієнтованого підходу, а не проблемно-орієнтованого з кримінальною розвідкою?*

За своєю суттю під час такої стадії управління ризиками, як ідентифікація ризиків, відбувається визначення ймовірних подій, які впливатимуть на здатність правоохоронного органу (або іншого суб'єкта контролю) виконувати завдання і функції для досягнення встановлених мети (місії) та цілей.

> *У чому полягає різниця між «ризиком» та «проблемою/проблемним питанням»?*

Ризик – це ймовірна подія, яка може виникнути в майбутньому, якщо зазначена подія все ж таки відбудеться - це може стати проблемою. Тобто ризик виникає в майбутньому, несе певну невизначеність та може відбутися/або не відбутися в якийсь час.

Водночас проблема/проблемне питання – це відома, існуюча або встановлена обставина, яка є або спричинила виникнення певних питань чи обмежень, що потребують вирішення. Іншими словами проблема – це обставина, що вимагає активних дій для усунення негативних наслідків, запобігання їх виникненню та потребує вивчення, дослідження і розв'язання.

Виходячи з цього, тактика кримінальної розвідки за логікою РОП, визначає спосіб реагування на кримінальну загрозу, зокрема яких заходів КР доцільно вжити, зумовлюючи їх зміст, послідовність, місце, час та інтенсивність проведення. Вона також передбачає вміння визначати напрям і характер дій у певній ситуації та раціонально здійснювати їх з огляду на їх особливості і поставлені завдання.

Через певні особливості деяких елементів тактики: оперативній комбінації, тактичним прийомам, утаємниченості самої діяльності, набором особливих прихованих інструментів впливу на фігурантів та процеси, що відбуваються у кримінальному середовищі, зашифрованого спостереження за ризиковими фігурантами та процесами тощо, може бути досягнуто реалізація одного із видів реагування на ризики це його мінімізація. Завдяки поєднанню тактики КР, системи аналізу ризиків, кримінального аналізу досягається синергія в управлінні ризиками, що значно підвищує результативність реалізації превентивної функції правоохоронного органу, а також сприяє підвищенню ефективності протидії кримінальним загрозам в економіці.

Превентивна тактика в контексті застосування РОП або управління ризиками по суті є інституціональним фрагментом, який характеризує логіку використання сил, засобів та методів ОРД з метою мінімізації ризиків.

До основних принципів, необхідних при розробці та реалізації загальної стратегії управління кримінальними ризиками, відносять: системність, безперервність, баланс відповідальності та ініціативи, поєднання аналітики і ризикової евристики, багатоваріантність, проактивність.



Характеризуючи в цілому весь арсенал методів управління ризиками національної, економічної та публічної безпеки, необхідно підкреслити їх конкретну практичну спрямованість, що дозволяє не тільки відібрати і проранжувати фактори ризику, але й змоделювати їх розвиток у майбутньому, оцінити з певною ймовірністю наслідки виникнення інцидентів, визначити зміни у характері кримінальних правопорушень, інших несприятливих ситуацій, а також підібрати методи міні-

мізації їхнього впливу, визначити власника ризику або запропонувати заходи, що компенсують ризики, простежити за динамікою криміногенних процесів і, нарешті, прискорити їхню зміну в бік декриміналізації суспільних відносин, зокрема детінізації економіки, транспарентності системи управління публічними фінансами. Метою управління ризиками національної, економічної та публічної безпеки є не тільки сприяння поглибленому аналізу факторів, що впливають на процес криміналізації суспільних відносин, але й підвищення ефективності управлінських рішень.

Методи управління ризиками національної, економічної та публічної безпеки можуть і повинні стати засобом ефективної реалізації концепції її забезпечення на всіх рівнях управління – національному та регіональному. Якісне управління ризиком підвищує шанси системи управління безпекою домогтися успіху в довгостроковій перспективі, значно зменшує небезпеку неефективної реалізації самої концепції.

Важливо не тільки виявити потенційні ризики національної, економічної та публічної безпеки, але й оцінити їхній вплив на різні сфери життєдіяльності, вчасно ухвалити рішення щодо зниження ризиків, причому здійснювати управління ризиками на всіх стадіях кримінального циклу, а також реалізації концепції й адекватно задокументувати процеси управління ризиками для наступного використання цих знань у подальшій практиці управління аналогічними процесами.

Основними цілями превентивного впливу на процес криміналізації суспільних відносин в результаті застосування РОП є:

1. Зниження рівня криміналізації суспільних відносин, зокрема тінізації економіки;
2. Зниження кількості кримінальних правопорушень в певній сфері;
3. Зниження масштабів втягуваності законослухняних громадян у сферу відносин з високими кримінальними ризиками (географічний фактор (охоплення регіонів), кількісний фактор (кількість суб'єктів, що використовують типові способи вчинення злочину в галузі чи виді діяльності тощо);
4. Зниження збитків, шкоди, зокрема сум втрат бюджету та об'єму розкрадань міжнародної технічної допомоги;
5. Розподіл зон компетенцій між суб'єктами контролю (власниками ризику) в процесі детінізації економіки;
6. Удосконалення механізмів і алгоритмів аналізу ризиків, а також форм, способів та інструментів реагування на ризик;
7. Забезпечення зростання індексу якості оперативного контролю за криміногенною ситуацією.

Як нами вже зазначалося раніше, процес управління ризиками припускає проведення певних кроків, у тому числі:

- *виявлення передбачуваних кримінальних ризиків у певній галузі, видах діяльності, діяльності державних установ тощо;*
- *аналіз і оцінка галузевих та об'єктових ризиків, ризик-послуг та ризик-рішень розпорядників бюджетних коштів, а також ризик-рішень суб'єктів контролю;*
- *вибір способів реагування на ризик та методів управління ризиками;*
- *застосування обраних методів;*
- *оцінку результатів управління ризиками.*

Управління ризиком здійснюється на всіх стадіях кримінального циклу протиправної діяльності за допомогою моніторингу, контролю та необхідних коригуючих дій. Здійснює це відповідний аналітичний підрозділ правоохоронного органу у тісній взаємодії з його іншими підрозділами, а також з іншими суб'єктами контролю (власниками ризику), що мають оперативні можливості, юридичні повноваження та компетентності щодо реагування на ризики.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон України від 06 груд. 2019 р. № 361-IX.
2. Про Бюро економічної безпеки України: Закон України від 28 січ. 2021 р. № 1150-IX. 3. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості»: Указ Президента України від 27 верес. 2021 р. №479/2021.
3. Forrester, Jay W. (1973). World Dynamics (sec. ed.). Cambridge, Massachusetts. Wright-Allen Press, INC.
4. Ризик. Застосування ризик-орієнтованого підходу для побудови імовірнісних структурно-логічних моделей виникнення та розвитку. URL: https://pidru4niki.com/1800010250884/ bzhd/rizik_zastosuvannya_rizik-oriyentovanogo_pidhodu_dlya_pobudovi_imovirnisnih_strukturno-logichnih_modeley
5. Беккариа Чезаре. О преступлениях и наказаниях: пер. с итал. Киев: Ин Юре, 2014. 240 с.

DOI: https://doi.org/10.36486/978-966-2310-66-5-26

Жорстоке вторгнення Росії в Україну змінило контекст кібербезпеки.

Голова британського національного центру кібербезпеки (NCSC) Лінді Кемерон

РОЗДІЛ 26
Кібервійна та форсайт кіберстійкості

Сергій Демедюк

КІБЕРВІЙНА І КІБЕРСТІЙКІСТЬ

Кібервійна не є новим явищем. Перше електронне повідомлення було надіслано в 1971 році; через п'ять років групи, відомі як Тигрові команди, спробували атакувати комп'ютери ICL і IBM у рамках експериментальної програми інформаційної безпеки Міністерства оборони Великої Британії [1]. Хоча значна частина цієї теми захищена державною таємницею, стає все більш очевидним, що ми маємо досвід чотирьох десятиліть кібервійни, з якої можна отримати політичні уроки та знання, незважаючи на те, що це часто називають застарілими термінами, такими як «інформаційна безпека» або «комп'ютерна безпека» [2; 3].

Термін «кібервійна», запроваджений Пентагоном на початку 1990-х років, спочатку став об'єктом значного скептицизму. Після закінчення холодної війни бюджети на оборону раптово зменшилися. Багато експертів з питань кібербезпеки вважали обговорення про «кібервійну» дещо безнадійною спробою оборонних відомств захистити виснажені бюджети. Ця нова загроза вимагала значних витрат на дослідження та розробки, які не були достатньо зрозумілі для парламентів. Скептицизм щодо реальності справжньої «кіберзагрози» значно зріс внаслідок очевидно обмеженого впливу, спричиненого помилкою тисячоліття Y2K, і зберігся у двадцять першому столітті [4; 5].

Вважається, що перша кібервійна відбулася в Естонії в 2007 році, а друга - в Грузії в 2008-2009 роках [6]. Коли у 2010 році Stuxnet успішно використали для паралізування ядерних центрифуг Ірану, він ще більше збудив кіберскептиків. Кібератака, спрямована на Іран, була здійснена за допомогою надзвичайно складного комп'ютерного хробака, спрямованого на певну конфігурацію промислового обладнання Siemens. Хоча ніхто офіційно не знав, хто створив Stuxnet, кілька ключових компонентів було виявлено. По-перше, він продемонстрував надзвичайний інтелект, вибірково заразивши кілька комп'ютерів за межами Ірану. По-друге, він продемонстрував здатність долати складні розриви та інші засоби захисту, що застосовуються іранською владою. По-третє, хробак Stuxnet використав не один, а кілька експлойтів «нульового дня» [7, с. 23].

У лютому 2014 року розпочалась російська збройна агресія проти України, яка велась також і в кіберпросторі. Майбутній директор американського Агентства національної безпеки Майкл Роджерс з цього приводу зазначав, що разом з військовою операцією із захоплення Криму, Росія розпочала проти України кібервійну[8]. Кібервійною називають російські атаки й українські експерти[9].

Після початку збройної агресії Російської Федерації проти України, компанії, що спеціалізувалися на наданні послуг кібербезпеки, стали реєструвати зростання кількості кібератак на інформаційні системи в країні. Зазвичай кібератаки були націлені на приховане викрадення важливої інформації, ймовірніше для надання Росії стратегічної переваги на фронті. Жертвами російських кібератак ставали урядові установи України, країн ЄС, Сполучених Штатів, оборонні відомства, міжнародні та регіональні оборонні та політичні організації, аналітичні центри, засоби масової інформації, дисиденти[10].

Лише щодо деяких з них:

> *на думку Адміністрації Президента США хакерська атака на Україну з боку Росії в червні 2017 року із використанням вірусу NotPetya стала найбільшою відомою хакерською атакою [11].*
>
> *12 грудня 2023 року у роботі найбільшого в Україні оператора зв'язку «Київстар» стався масштабний збій. По всій країні у абонентів «Київстар» зник мобільний зв'язок та інтернет, при цьому користувачі не могли і приєднатися до мереж інших операторів у рамках внутрішньо українського роумінгу [12]. Також припинили роботу сайт та застосунок «Київстару». Зв'язок зник у 24 мільйонів абонентів [13]. Збої виникли у всьому обладнанні, яке використовувало зв'язок «Київстар», що призвело до серйозних інфраструктурних проблем по всій Україні [14].*

Загалом, згідно з аналітичним звітом Держспецзв'язку України за I півріччя 2023 року, лише упродовж січня-червня 2023 року кількість кібератак проти України зросла до 762 зареєстрованих інцидентів, що більше ніж удвічі за показники II половини минулого року [10].

Водночас більшість статистичних даних про кіберзлочинність піддаються сумніву.

Наприклад, професор Пітер Зоммер, професор Лондонської школи економіки, стверджує, що деякі недавні державні звіти про кіберзлочинність фактично виступають лише «інструментом для спонукання до продажу» для спеціалізованих компаній, які займаються безпекою. Він назвав звіт Detica «прикрим надуванням» [15]. Зоммер стверджує, що до цього часу ще не досягнуто згоди щодо конкретного вмісту розрахунку збитків.

Тайлер Мур, експерт з кібербезпеки Гарвардського університету, пояснює, що причина складності отримання точних оцінок полягає у тому, що не завжди повідомляють про всі випадки. Жертви не охоче зізнаються в порушенні безпеки, а в деяких випадках навіть не знають, що на них було скоєно напад [16].

На цей час одна з ключових проблем у кіберстійкості пов'язана з недостатнім розвитком освіти у сфері безпеки IT. Також потрібні культурні зміни, оскільки менше IT-експертів просуваються до найвищих посад компаній, які не входять до технологічного сектору, і їх недостатньо в урядовому багатті.

Кібервійна містить хвилюючий феномен. Передові суспільства, які розвинули ці можливості, якраз і є найбільш вразливими до електронної війни. На противагу цьому, кібератака на Кубу, яка має один з найнижчих показників використання комп'ютерів у світі (17 користувачів на 1000 осіб) і нерозвинену цифрову інфраструктуру, матиме відносно невеликий вплив [1]. Країни Організації економічного співробітництва та розвитку (OECD) дедалі більше залежать від цифрових систем в управлінні своєю життєво важливою інфраструктурою [17]. SCADA-системи, спеціально розроблені для контролю промислових процесів, можуть дистанційно керувати компонентами водопостачання, енергетики, транспорту та зв'язку. Stuxnet був створений з метою нападу на SCADA-системи і недвозначно показав, що деякі з таких систем можуть бути пошкоджені, що може призвести до значних наслідків. Більше того, точний масштаб загрози і необхідний захист залишаються непрозорими [1].

До цього часу, урядовці вважали, що критична інфраструктура розвинених країн може бути захищена шляхом використання все більш вдосконалених технічних рішень. Тим не менш, Stuxnet підтвердив, що більшість цифрових систем, незалежно від їхнього високого рівня захисту, все одно є вразливими.

Отже, щоб запобігти кібератакам, можливо, потрібно використовувати аналогові системи для моніторингу запасу електроенергії, води та інших важливих комунальних послуг. Наразі, занепокоєння можливістю кібератак на атомні електростанції вже призвело до свідомого урізноманітнення систем з поєднанням цифрових, аналогових і ручних [1]. Однак у двадцять першому столітті зробити це в основній інфраструктурі надзвичайно складно, оскільки інженери звернулися до цифрових рішень для підвищення операційної ефективності [18].

Наприклад, інфраструктуру Великої Британії не можна вимкнути, як вимикач, частково тому, що вона все ще має певну «системну різноманітність». Частково це результат застарілих систем, а частково - результат випадковості. Небезпека полягає в тому, що це ненавмисне, але цінне джерело стійкості буде знищене в ім'я скорочення витрат і підвищення ефективності. Широке впровадження інтелектуального обліку є прикладом універсальної системи, яка містить вразливість, зумовлену прагненням до більшої ефективності та результативності [1].

Отже, різноманітність систем стала новим улюбленим словом у сфері кібербезпеки.

> *Стійкість вимагає дедалі складнішого поєднання фізичної безпеки, безпеки персоналу, контролю закупівель і зміцнення систем разом з подальшими заходами для запобігання несанкціонованим або ненавмисним модифікаціям дизайну системи безпеки.*

Крім того, впровадження злагоджених аналогових і людських систем безпеки суттєво змінило уявлення про інформаційну безпеку. До цього моменту спеціалісти з інформаційної безпеки головним чином займалися кіберзлочинністю, зазвичай проводили складні спроби проникнення в системи безпеки банків і великих компаній. За більш ніж 10 років роботи в цій сфері було зроблено висновок, що більшість збоїв у системі безпеки є наслідком поєднання людської некомпетентності та зловмисності [19, с. 1]. Однак, зважаючи на загрозу серйозної кібервійни на державному рівні, експерти розглядають людей разом із системами як останню лінію захисту від витончених кібератак [1].

Серед фахівців з інформаційної безпеки була поширена ортодоксальна думка, що головною перешкодою для безпеки системи є люди, а не самі системи [20]. Вірогідною була думка, що більшість серйозних порушень безпеки виникають через недостатній рівень знань персоналу, а не через технічні неполадки. Проте поява комп'ютерного хробака Stuxnet, який був використаний для нападу

на ядерні центрифуги в Ірані, вказує на те, що такий підхід має бути переглянутий. Велика кількість людей почала вивчати майбутню кібербезпеку після виявлення складного шкідливого програмного забезпечення, яке шпигує за промисловими системами та підриває їх.

Відповідь на питання кіберстійкості, як у випадку Stuxnet, полягає в поєднанні різноманітних або гібридних систем, які керують певною частиною національної інфраструктури. У той час навіть найбільш захищені системи могли бути піддані технічним атакам іззовні. У наступні десятиліття основним каталізатором інформаційно-комунікаційних технологій стане все ближчий зв'язок між інтернетом і людьми. Головною ціллю комерційних технологічних підприємств є безперешкодне об'єднання людини та інтернету. На сьогодні це виявляється в потужніших портативних пристроях, сполучених з хмарними технологіями.

Однак, майбутнє просунутого зв'язку між людиною та інтернетом – це прямий інтерфейс між комп'ютером і мозком, сфера, в якій медичні технології вже розширюють межі [21]. Вплив цього розвитку на кіберстійкість має певну вагу. Коли людина буде відправляти електронне повідомлення, «після роздумів і короткого кліпання очима» [1], кібербезпека стане ще важливішою, ніж на сьогодні. Щоб захистити нашу інфраструктуру, ми повинні докладати рішучих зусиль, щоб впоратися з комерційними та культурними перешкодами, спрямованими на надмірну залежність від електронних систем.

Витрати на інтернет-безпеку також створюють серйозні труднощі, але в значно більшому розмірі. Це надзвичайно дорога і ризикована сфера, ніхто по-справжньому не хоче нею володіти [1]. Однак більшість людей погоджується, що інтернет має вирішальне значення, і що його потрібно захистити.

Управління кібербезпекою є типовим прикладом міжурядової сфери, яка працює на регіональному рівні значно краще. У Європі існує власна кібер-організація, Європейське агентство з мережевої та інформаційної безпеки (European Network and Information Security Agency - ENISA), розташована на острові Кіпр. У практичній сфері ENISA виконує функцію координації регулювання та сприяє зближенню, але має обмежені можливості оперативних дій. Тим не менш, більшість ІКТ-бізнесу позитивно ставиться до ENISA, стверджуючи, що один набір регуляторних практик для Європи є кращим, ніж 26 [22]. Масштаби телекомунікаційної галузі означають, що саме Європейське агентство, а не уряд, має більший операційний потенціал і, власне, досвід для забезпечення значущої кіберстійкості [1].

Будучи за своєю природою транснаціональними і часто використовуваними у контексті глобалізації, агентства Європейського Союзу, такі як ENISA, також мають схожі проблеми складності і невизначеності, які ставлять у скрутне становище національні уряди. Кіберстійкість може бути найбільш привабливою через те, що вона може використовуватися як рухома ціль. У тривалий період часу урядові програми та проекти не досягали успіху. Це було пов'язано з тим, що вони були надто вибуховими та не мали потенціалу для впровадження нових технологій, а також тому, що приватний сектор розвивався швидше, ніж уряд. Що ми знаємо напевно, так це те, що світ інформаційно-комунікаційних технологій прискорюється, а проблеми, які стоять перед урядом, зростають у своїх розмірах і складності [1].

Отже, в майбутньому враховуватиметься гібридизація процесів розвідки, безпеки, ризиків і стійкості для досягнення кіберстійкості ландшафту. Однак, короткостроково, це стає проблемою для управління, як з точки зору власності, так і з точки зору співпраці між державними й приватним секторами.

МЕТОДИ ТА СИСТЕМИ ФОРСАЙТУ КІБЕРСТІЙКОСТІ

Форсайт – це складний, багатоетапний та безперервний процес, кінцевою метою якого є прийняття обґрунтованих рішень щодо забезпечення стратегічних планів для можливого різноманітного розвитку подій у майбутньому. Він дає змогу осмислити різні можливі варіанти майбутнього та стратегічно підготуватися до ймовірних сценаріїв. З середини 1950-х – початку 1960-х років форсайт як дисципліна перетворився на основний інструмент стратегічного планування як для приватних корпорацій, так і для державного сектору [1].

Форсайт продовжує розвиватися й змінюватися і сьогодні. Це значною мірою пов'язано з тим, що

він орієнтований на дії, а отже, має відчутні результати;

він є відкритим, тобто в рамках форсайту існує свобода мислити нестандартно або переосмислювати попередні уявлення;

нарешті, він є міждисциплінарним, він об'єднує різні групи, які мають досвід у широкому діапазоні тем, таким чином забезпечуючи більш реалістичне і продумане можливе майбутнє.

У виданні ЄС «Що таке форсайт» зазначається:

> *«Форсайт – це не пророцтво і не передбачення. Він не має на меті передбачити майбутнє – розкрити його так, ніби воно визначене наперед, – а допомогти нам його побудувати» [23].*

Виділяють три основні переваги форсайту [24, 25]:
- *генерація знань,*
- *сприяння відносинам із зацікавленими сторонами,*
- *посилення спроможності.*

Знання допомагають окремим зацікавленим сторонам найкращим чином позиціонувати себе для майбутнього розвитку; маючи знання, вони можуть бачити поза оманою, що майбутнє буде схожим на теперішнє, і уявляти собі передове майбутнє [24]. Розвиток таких знань і розуміння сприяє підвищенню зв'язків між зацікавленими сторонами, що у свою чергу посилює мережі, особливо у випадку кібербезпеки.

Форсайт сприяє посиленню спроможностей; результати форсайту дозволяють визначити, що є важливішим для організаційних спроможностей і спроможностей зацікавлених сторін. Визначення та підтримка цієї інформації є життєво важливими для розвитку та отримання ключових навичок, технологій та політики.

Застосування форсайту у сфері кібербезпеки наразі не є широко розповсюдженим [26]. Проте, запровадження зазначених методів в галузь кібербезпеки сприятиме набуттю ще більш глибокого, розумного та взаємодіючого усвідомлення ризиків, а також стратегічних наслідків заходів забезпечення безпеки.

> *Щоб адекватно реагувати на майбутні загрози кібербезпеці та формувати більш безпечне суспільство, необхідно спиратися на висновки та дослідження спільноти фахівців з питань майбутнього та форсайту, щоб розробити процес застосування форсайту до кіберстійкості.*

Для досягнення здатності розуміти можливості майбутнього, важливо належним чином розвивати кібербезпекову екосистему з метою вирішення та управління новими та майбутніми викликами.

Як кіберстійкість, так і форсайт отримують вигоду від багатогранного і міждисциплінарного середовища. Часто розумно об'єднувати системи з інших галузей з цієї самої причини. Вважається [24], що керівні принципи, практики, підходи, методи та інструменти як системного мислення, так і розробок, орієнтованих на користувача, можуть бути ключовими для формування правильного мислення [27] при підході до форсайту у сфері кібербезпеки.

Для того, щоб краще проілюструвати спектр методів, відповідні методи, системи та інструменти, як правило, групуються в шість категорій [28]. Тим не менш, не всі прийоми можна визнати характерними для передбачення майбутнього. Також використовуються стратегічні методи планування та методи вирішення проблем, які часто включаються у діяльність форсайту.

Загалом, виділяються такі групи методів [23]:
- *системи аналізу середовища*
- *аналіз тенденцій*
- *форсайт експертні групи*
- *сценарний метод*
- *морфологічний аналіз та ретроспективний аналіз*
- *методи аналізу кібербезпеки.*

Системи аналізу середовища дають користувачам можливість ретельно вивчати обране середовище для виявлення слабких сигналів вхідних змін, які можуть мати значний вплив на майбутнє. Ці методи сприяють структурованому та аналітичному сприйняттю поточної ситуації з метою досягнення взаєморозуміння. Зазвичай, ці методи базуються на засадах діагностики.

Існують різні методи для сканування середовища, серед яких, наприклад, такі:

STEEP *– система аналізу соціокультурних, технологічних, економічних, екологічних та політичних факторів певної сфери;*

PESTLE *– система аналізу політичних, економічних, соціокультурних, технологічних, правових та екологічних факторів певної сфери.*

SWOT *– система визначення та аналізу сильних і слабких сторін, можливостей і загроз для певного напряму або організації.*

Кожна з перерахованих систем дозволяє проводити систематичну оцінку характеристик, змін і впливів у зазначених областях, щоб отримати уявлення про навколишнє середовище.

Крім того, існують інші відмінності цих ідей, які враховують інші сфери - вибір методу або сфери має ґрунтуватися на початковому аналізі цієї теми.

Аналіз тенденцій. Тенденція визначається певним трендом змін в часовому вимірі або появою нової моделі змін, яка зазвичай впливає на великі соціальні групи [29]. Методи аналізу тенденцій зазвичай слугують прогностичним або діагностичним цілям.

Тренди можна аналізувати різними способами – наприклад, за допомогою оглядів літератури, бібліометрії, текстового аналізу, патентного аналізу та аналізу впливу трендів. Ці методи виявляють поточні або нові тенденції і, як правило, досліджують причину, потенційний вплив, ймовірність і швидкість виникнення цих тенденцій [30].

Інші методи, що використовуються для аналізу тенденцій, включають [23]:

- ✓ *причинно-наслідковий багаторівневий аналіз – сприяє визначенню рушійних сил шляхом отримання розуміння сприйняття учасників, таких як світогляд, цінності та культурні норми;*
- ✓ *тренд-радар – надає міжгалузевий погляд на нові та вже існуючі тенденції в цільовому середовищі;*
- ✓ *аналіз впливу трендів – аналіз впливу однієї або декількох можливих подій на екстраполяцію тренду в майбутнє;*
- ✓ *сканування горизонту – систематичний моніторинг поточних тенденцій, а також виявлення нових, актуальних подій у певній сфері за допомогою творчого процесу колективного осмислення.*

Форсайт-експертні групи охоплюють широкий спектр методів і підходів. Експертні панелі та метод Дельфі є одними з найвідоміших складових сімейства форсайт-експертних груп. У обох випадках експерти висловлюють свою думку про майбутнє. Проте метод Дельфі полягає в більш структурованому підході до спілкування, щоб отримати відповіді від фахівців. Експерти зазвичай запрошуються для підтримки проекту з форсайту з прогнозними або рекомендаційними цілями.

> ***Дельфі** – це дослідницький метод, заснований на структурованому та ітеративному груповому спілкуванні між експертами, які висловлюють судження з обраної теми. У першій послідовності різні експерти в певній галузі опитуються окремо щодо конкретної теми або питання. Потім збираються їхні анонімні відповіді, і експертів просять прокоментувати зібрані думки. Для досягнення консенсусу цей процес повторюється кілька разів. Такий підхід допомагає уникнути групового мислення, а отже генерує більше креативних ідей з різних точок зору. Весь процес можна проводити дистанційно, що полегшує залучення більш різноманітної групи експертів з усього світу. Цей метод може забирати багато часу, особливо коли є кілька ітерацій [23].*

Японський національний інститут науково-технічної політики (NISTEP) проводить форсайт приблизно кожні п'ять років, більшість з яких ґрунтується на великому дослідженні за методом Дельфі, в якому беруть участь близько 2000 учасників [31].

Інші приклади методів, заснованих на експертних групах, включають [23]:

- ✓ *зведені судження / груповий прогноз – логічно поєднує декілька індивідуальних суджень в узгоджені та колективні судження;*
- ✓ *дослідження ключових технологій (технологічне прогнозування) – застосовує набори критеріїв до критичних технологічних розробок з метою надання обґрунтованої оцінки.*

Водночас існують також методи колективного форсайту, за яких інформація збирається у не експертному середовищі.

Сценарні методи. Серед найбільш поширених і відомих методів передбачення у форсайті є сценарні методи. Вони використовуються як інструменти дослідження для розмірковування про можливе, бажане або небажане майбутнє, але не для точного передбачення конкретного майбутнього. Крім того, ці методи можуть бути використані для створення та оцінки різних варіантів, щоб знайти найкращий підхід. Зазвичай вивчається кілька можливих сценаріїв майбутнього, щоб прийняти рішення, які можуть допомогти запобігти потенційним проблемам і пасткам.

Зазвичай на початку розробки сценаріїв проводиться діагностика, яка дозволяє об'єктивно розглянути основні фактори, що можуть вплинути на майбутнє питання, яке вивчається. Розгляд кількох потенційних варіантів майбутнього підвищує розуміння різних факторів, що можуть впливати на майбутнє. Ці знання дозволяють створити більш гнучкі, перспективні та адаптивні рішення.

Наприклад, сценарії можна розробляти різними методами [23]:

- ✓ *ігри – розробка ігор або рольових сценаріїв для тестування можливих стратегій або рішень шляхом визначення можливих реакцій та наслідків їх реалізації;*
- ✓ *візія – погляд в ідеальне майбутнє для створення стратегії досягнення конкретних цілей;*
- ✓ *аналіз перехресного впливу – оцінює ймовірність настання певних подій у майбутньому шляхом оцінки ймовірності настання інших подій, а потім досліджує їхній взаємний зв'язок.*

Морфологічний та ретроспективний аналіз. Ця група включає в себе різноманітні методи, які зазвичай не мають взаємозв'язку, але мають однакові дві характеристики – намір передбачення та акцент на регресію подій і декомпозицію системи. Регресійний аналіз у форсайті дотримується

підходу, подібного до статистичного регресійного аналізу. Однак регресійний аналіз у форсайті працює з якісними даними й суб'єктивною думкою, на відміну від кількісних методів визначення подій і тригерів подій, які можуть призвести до передбачуваної майбутньої події [32]. Однак декомпозиція ставить за мету розділення складних систем на менші компоненти для полегшення аналізу їх структури, динаміки взаємодії та впливу на систему в цілому.

> ***Морфологічний аналіз*** *– це творчий, евристичний, нормативний метод, який підтримує дослідження складних проблем і можливих рішень за допомогою багатовимірної матриці [23].*

Це трудомістка групова вправа, яка потребує фасилітації [33].

> ***Бек-кастинг*** *– ще один нормативний метод, який фокусується на обраному сценарії бажаного (або небажаного) майбутнього. Потім учасники рухаються назад у часі, щоб визначити рішення або події, які мають відбутися, щоб перетворити обраний сценарій на реальність [23].*

За допомогою беккастингу організації можуть планувати, дії що їм слід вжити, та оцінювати потенційні наслідки. Це підвищує обізнаність про те, що майбутнє визначається багатьма факторами і що різні дії призводять до різних альтернативних результатів [33].

> ***Прогнозування загроз*** *– це багатоетапний метод, який передбачає уявлення небажаного майбутнього, а потім реконструкцію кроків і рішень, які необхідно вжити, щоб запобігти цьому майбутньому [23].*

Він був розроблений, перш за все, для аналізу військового майбутнього. Прогнозування загроз поєднує в собі багато методів передбачення, включаючи Дельфі, науково-фантастичне прототипування, беккастинг і моделювання сценаріїв. Цей метод має визначений часовий горизонт – кожна діяльність спрямована на 10 років вперед [34].

Інші методи, що входять до цієї групи [23]:

- ✓ *аналіз технологічної послідовності – генерує імовірні часові рамки для технологічних послідовностей шляхом аналізу оцінок часу, необхідного для проміжних технічних кроків;*
- ✓ *розробка дорожньої карти – розробляється документ, який визначає кроки та етапи, необхідні для досягнення бажаного майбутнього;*
- ✓ *багатокритеріальний аналіз – порівнює можливі ідентифіковані рішення із зваженим набором критеріїв оцінки;*
- ✓ *синектика – сприяє новому і творчому мисленню, наприклад, уявляючи обрану проблему в незвичному, не пов'язаному з нею середовищі.*

Методи аналізу кібербезпеки. Кібербезпека є складовою системи, яка включає розгляд інцидентів і криз, а також ретельний аналіз майбутніх ризиків і загроз. Усі ці способи є різновидами способів оцінювання ризиків. Хоча фокус кожного з них трохи відрізняється (наприклад, на суб'єкті загрози або на візуалізації), загальна мета кожного з них полягає в тому, щоб знайти та визначити пріоритети ризику, а потім прийняти відповідні заходи. Цей підхід може бути використаний для постановки діагнозу, прогнозування або надання рекомендацій.

Найвідомішими методами, які добре себе зарекомендували в аналізі ризиків і моделюванні загроз є такі:

- ✓ *оцінка ризику агента загрози (Threat Agent Risk Assessment (TARA) [35] – метод оцінки ризиків на основі загроз, який використовується для виявлення, оцінки та визначення пріоритетності ризиків. Він зосереджує увагу на суб'єктах загроз, їх мотивації та можливих методах;*
- ✓ *оперативно критична оцінка загрози, активу і вразливості (Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) [36] – комплексний метод оцінки для виявлення, ранжування та управління ризиками кібербезпеки;*
- ✓ *моделювання загроз [37] – метод концептуального аналізу, що використовується для виявлення потенційних вразливостей і розробки заходів на ранніх стадіях розробки додатків або послуг. Існує багато систем і методів для моделювання загроз, одним з таких методів є Дерево атак. Дерева атак базуються на визначенні дерев можливих методів, які можуть допомогти зловмиснику досягти своїх цілей.*

Інструменти. Незважаючи на те, що вони не повністю ідентичні, інструменти є платформами або допоміжними системами, які допомагають у застосуванні методів прогнозування. Незважаючи на те, що деякі з них спрямовані на оцифрування форсайту, інші лише мають на меті покращити ваш досвід форсайту на індивідуальному рівні. Під час вибору інструментів форсайту для конкретної діяльності слід розглянути інші потенційні джерела, оскільки деякі з них спеціально розроблені для певної аудиторії або ситуації.

Інструменти для фасилітації семінарів часто використовуються фасилітаторами воркшопів для полегшення комунікації під час воркшопів або для генерування креативних ідей від учасників. Ось кілька відомих прикладів [23]:

- ✓ *мозковий штурм, коли учасників заохочують генерувати велику кількість сирих, спонтанних ідей, надихаючись ідеями інших учасників, без негайного оцінювання;*
- ✓ *світове кафе, де велика група учасників може обговорити різні питання в структурований спосіб, по колу, в менших групах, і записати свої ідеї на великих аркушах паперу, щоб інші групи могли бачити й використовувати їх як довідник;*
- ✓ *Mind mapping – метод графічної фасилітації, який допомагає візуально організувати зібрану інформацію.*

Існує кілька *цифрових баз даних*, які надають інформацію про інструменти, що стосуються форсайту. Одним із джерел для визначення додаткових інструментів для форсайту є веб-сайт Service Design Tools [38], який описує та впорядковує інструменти на основі етапу процесу проектування, зацікавлених сторін та учасників, мети діяльності та бажаних методів візуалізації. Інші ресурси включають Платформу майбутнього (Futures Platform) [39], Інструментарій майбутнього врядування (Governance Futures Toolkit) [40] та Teach the Future [41], який має на меті надати викладачам інструменти для інтеграції форсайту в їхні навчальні програми.

Інструменти на основі штучного інтелекту (ШІ) можуть допомогти в таких видах форсайту, як оцінка поточного середовища, аналіз тенденцій або екстраполяція тенденцій. Хоча ці інструменти не є повсюдними, вони часто інтегровані в процес форсайту [42]. Особливо корисним є використання ШІ для пошуку текстів й аналізу великих обсягів даних, таких як виявлення термінів і фраз, які вказують на нові або майбутні тенденції, або для підтримки огляду літератури. У більшості випадків для цього застосовується обробка реальної мови. Також інструменти, що базуються на штучному інтелекті, можуть допомогти у виборі сценаріїв.

Інструменти співпраці та форсайту / бази даних трендів. Для кращого полегшення форсайту багато експертів рекомендують використовувати інструменти для спільної роботи (наприклад, цифрові дошки і додатки для нотаток), а також дослідницькі бази даних для камеральних досліджень і розпізнавання тенденцій. Важливо зазначити, що в експертному середовищі не завжди довіряють існуючим радарним базам даних та джерелам інформації для форсайту. Ці джерела рідко публікують деталі процесу збору та підготовки інформації, тому опитані експерти, як правило, покладаються на власні дослідження або першоджерела для визначення інформації, пов'язаної з трендами.

Інструменти для проведення конференцій часто використовуються для залучення учасників з різних географічних регіонів. Вони надзвичайно корисні для об'єднання різноманітних груп учасників. Однак, використання цих інструментів має і зворотний бік. Учасники можуть бути менш здатними повністю присвятити свою увагу онлайн-зустрічам (на відміну від особистих семінарів) через меншу інтерактивність віддалених семінарів і той факт, що деякі учасники можуть піддаватися спокусі робити кілька справ одночасно або приєднуватися до інших зустрічей. Крім того, рівень цифрової грамотності в групі може бути різним – через брак технічних навичок та обізнаності деякі учасники можуть бути не в змозі повноцінно та впевнено брати участь під час використання інструментів для проведення конференцій.

ФОРСАЙТ КІБЕРСТІЙКОСТІ

Поява нових загроз є складною, швидкоплинною та іноді непередбачуваною подією, особливо з урахуванням стрімкого приросту кіберінцидентів. Отже, часто може статися, що ймовірність та актуальність окремих загроз у багатьох випадках може раптово змінитися через непередбачувані інциденти, суспільні зміни або спонтанні інновації. Різнобічні глобальні ініціативи охоплюють широкий спектр тем, включаючи визначення кіберзагроз та класифікацію їх за рівнем небезпеки. Багато загроз, відомих сьогодні, залишаться актуальними в майбутньому, але їх характер зміниться через зростання залежності, демократизацію та розвиток нових технологій.

Прикладом системної роботи з визначення майбутнього (форсайту) у сфері кібербезпеки є проведений аналіз за ініціативою ENISA у період з березня по серпень 2022 року [43], яким було визначено та ранжовано 21 загрозу, поширеність яких зростатиме до 2030 року. Було проведено серії семінарів та інтерв'ю з відповідними експертами за методом PESTLE та застосовано різноманітні підходи до методології.

Використана методологія ENISA складається з чотирьох етапів [24].

Перший, «*спільне дослідження*», – це фаза дослідження тенденцій та збору інформації, яка інтегрувала знання експертів, зворотний зв'язок та перевірку.

На другому етапі, «*групові семінари з прогнозування*», збиралися групи експертів з досвідом роботи в одному з вимірів PESTLE для подальшого обговорення, вивчення, оцінки та визначення пріоритетів виявлених тенденцій.

Третій етап, «*ідентифікація загроз*», ґрунтувався на методології «кастингу загроз» для визначення нових викликів, які можуть виникнути впродовж наступних 10 років. Для цього невеликим групам експертів з кібербезпеки надавався сценарій, який поєднував пріоритетні тенденції.

На наступному етапі, визначені учасниками-експертами, *загрози були оцінені* за такими показниками, як імовірність, вплив, новизна і те, чи була ця загроза раніше визначена. Новизна розглядалася для того, щоб визначити пріоритетність менш відомих загроз.

Акцент було зроблено на 10 кіберзагрозах з найвищим рейтингом, при цьому, суб'єктами загроз визначено чотири основні групи: держава-спонсор, кіберзлочинці, хакери-найманці та хактивісти [44].

Методологічно прогноз побудовано на основі поточної таксономії загроз ENISA [45], яка поділяє їх на такі категорії високого рівня:

- *фізична атака (навмисна),*
- *ненавмисне пошкодження / втрата інформації або IT-активів,*
- *стихійні лиха (природні),*
- *збої / несправності,*
- *перебої в роботі,*
- *підслуховування / перехоплення / викрадення,*
- *недобросовісна діяльність / зловживання, а також правові аспекти.*

Важливо зазначити, що ненавмисні загрози розглядаються як вразливості, які можуть бути використані суб'єктом загрози, а тому основний акцент зроблено на навмисних загрозах [24]:

- ✓ *компрометація ланцюжка поставок програмних засобів;*
- ✓ *просунуті кампанії з дезінформації / операцій впливу;*
- ✓ *зростання авторитаризму цифрового нагляду / втрата приватності;*
- ✓ *людські помилки та застарілі системи в кіберфізичних екосистемах;*
- ✓ *цілеспрямовані атаки (наприклад, програми-вимагачі), посилені даними зі смарт-пристроїв;*
- ✓ *брак аналізу та контролю космічної інфраструктури та об'єктів;*
- ✓ *зростання сучасних гібридних загроз;*
- ✓ *дефіцит навичок;*
- ✓ *транскордонні постачальники послуг ІКТ як єдина точка відмови*
- ✓ *зловживання штучним інтелектом.*

Надамо коротку характеристику цим ключовим загрозам у кіберпросторі.

Компрометація ланцюжка поставок програмних засобів. До 2030 року все більшою буде інтеграція компонентів і сервісів, об'єднаних у нові продукти. Оскільки ринок вимагає швидких циклів випуску продуктів, програмування на основі компонентів значно зросте [46], що призведе до повторного використання коду та використання бібліотек коду з відкритим вихідним кодом.

Незважаючи на регулярну перевірку деяких з цих компонентів на вразливості, поєднання програмного, апаратного та компонентного коду створюватиме неконтрольовані взаємодії та інтерфейси [47]. З'являться нові та непередбачувані вразливості, що дасть кіберзлочинцям більше шансів порушити ланцюг постачання як з боку постачальника, так і з боку клієнта.

Потенціал використання вразливостей програмного забезпечення, атак на конфігурацію програмного забезпечення та апаратного забезпечення, фішингових атак й ін'єкцій шкідливого програмного забезпечення в бібліотеки коду є політичними та фінансовими мотивами цих суб'єктів. Це може призвести до серйозних проблем у ланцюгах постачання й використовується зловмисниками для здійснення політичних дестабілізацій, фінансового маніпулювання або шпигунської діяльності.

Злочинці можуть керувати інструментами розробки та програмними залежностями, вставляючи бекдори до складових коду. Бібліотеки з відкритим кодом є одним із найпростіших способів, якими злочинці можуть користуватися. Зловмисники можуть отримати початковий доступ до комерційних застосунків за допомогою різних методів, наприклад, компрометації «drive-by» або атаки, які використовують соціальну інженерію. Запуск троянських програм, дроперів або руткітів у програмні компоненти, які надаються, дозволяє зловмисникам отримати доступ до мережі їхньої кінцевої цілі, що залежить від апаратних або програмних компонентів організації [24].

Також можливий фізичний вплив на апаратне забезпечення на виробничих потужностях. Для того, щоб такі злочинці могли втілити свій замисел, вони мають отримати фізичний доступ (або, принаймні, бути в безпосередній близькості) до приміщень виробництва апаратних компонентів. Злочинці могли б потрапити на законні об'єкти шляхом використання особи зсередини, яка б працювала там і мала б ідеальний доступ до апаратного забезпечення для компрометації даних або системи.

Іншим випадком може бути компрометація широко використовуваної приватної компанії з доступом до конфіденційних даних [48].

Просунуті кампанії з дезінформації / операцій впливу. У 2030 році окремі суб'єкти, такі як злочинні угруповання, наймані хакери, а також держави-спонсори, імовірно, матимуть доступ до нових технологій, таких як діпфейки, для розширення своїх зловживань і маніпуляцій суспільством шляхом поширення дезінформації. Незважаючи на те, що використання технології діпфейк може призвести до незаконного збагачення окремих осіб або злочинних угруповань, основна мета дезінформаційних кампаній з використанням підроблених ідентичностей зазвичай є геополітичною, і, швидше за все, їх ініціаторами є окремі держави та інші політично мотивовані групи [24].

Джерел даних зараз незліченна кількість; противники можуть тренувати свій ШІ для глибоких фейкових атак [49], використовуючи широкий спектр загальнодоступних відео, фотографій і записів голосу людей (навіть тих, хто не є публічною особою). Біометричні зображення обличчя особливо вразливі до морфінг-атак (morphing attacks), в яких зловмисник може з високим ступенем точності видавати себе за свою ціль. Технологія глибокої підробки також може створювати нереальні обличчя [50], які людське око не в змозі відрізнити від справжніх. Тобто виникає можливість створення реалістичних аватарок, які відрізняються від уже складних ботів у соціальних мережах. Крім того, майбутні боти, які мають здатність впливати на вибори та формувати довіру громадськості, будуть публікувати свої відео в соціальних мережах та активно брати участь у дебатах. За допомогою штучного інтелекту, аналізу тексту або голосу можна ще більше посилити дезінформаційні кампанії, щоб забезпечити індивідуалізовані відповіді окремим особам.

Зростання авторитаризму цифрового нагляду / втрата приватності. Злочинців все частіше ідентифікують за допомогою таких технологій, як відстеження місцезнаходження, громадські камери та розпізнавання обличчя [51]. У майбутньому це може спонукати держави, а також приватних суб'єктів, значно розширити використання цих технологій. Через такі технології, як розпізнавання обличчя у публічній сфері, посилення цифрового нагляду на інтернет-платформах або запровадження цифрової ідентичності, індивідуальні свободи можуть бути обмежені заради безпеки та захисту. Доступ до цих даних дозволить правоохоронним органам та іншим державним установам відстежувати потенційних підозрюваних і заохочуватиме їх до цього. Ці сховища даних також можуть стати величезною мішенню для злочинних угруповань, які зможуть продавати в інтернеті дані про особу на основі однієї лише фотографії [24]. Приватний сектор також відіграє важливу роль, особливо коли основні технології розпізнавання обличчя або контент-платформи знаходяться під контролем одного лідера ринку. Провайдери, які надають технології розпізнавання обличчя або контент-платформи, стануть мішенню для величезних масивів консолідованих даних голосу та зображень. Крім того, дії приватних корпорацій не завжди можуть відповідати вимогам захисту даних і безпеки.

Уряди (в тому числі правоохоронні органи) й приватні підприємства в рамках державно-приватного партнерства можуть в межах своїх правових норм законно збирати персональні дані, в тому числі біометричні дані. Це створює виклики [52] для регуляторних органів і громадськості, щоб забезпечити дотримання законів, які захищають їхнє приватне життя. Крім того, це вимагає від усіх суб'єктів, які збирають ці дані, мати необхідні механізми захисту. Як тільки зловмисники отримують доступ до мережі, вони можуть почати автоматизований збір даних, потенційно використовуючи інтерпретатор команд і сценаріїв, а також API, інтерфейси командного рядка або сервіси вилучення, перетворення й завантаження (ETL) в хмарних середовищах. Одним із варіантів використання може бути зловживання зібраними даними правоохоронними органами або онлайн-спільнотами для відстеження потенційних злочинців [24].

Поява інтерфейсу між комп'ютером і мозком також ознаменує остаточне зникнення розриву між кібербезпекою і розвідкою. Ми добровільно розміщуємо величезні обсяги даних в Інтернеті, і багато з наших повсякденних дій залишають за собою електронний слід. Наш набір публічних і приватних даних містить широкий спектр інформації та включає в себе все – від покупок за кредитними картками й бібліотечних книг до «оновлень статусу», які ми охоче публікуємо на платформах соціальних мереж. За останні 10 років одним з найважливіших досягнень у сфері спостереження стала можливість видобувати дані з цих величезних пилових пагорбів тривіальних, на перший погляд, даних для отримання розвідувальної інформації, яка має все більшу цінність. Показово, що служби технічної розвідки зараз інвестують менше грошей в криптографію і більше – в зберігання даних і великомасштабну обробку даних [1].

Водночас існує і альтернативна точка зору щодо поглинання приватності. У 1998 році Девід Брін опублікував інтригуючу книгу під назвою «Прозоре суспільство». Недооцінена під час першої публікації, ця маленька класика є однією з найбільш інтригуючих дискусій про наше цифрове майбутнє. Він стверджує, що, хоча приватність добігає кінця, ми не повинні надмірно перейматися цим питанням. Він наполягає на тому, що насправді важливо, хто володіє даними і як ними керує. Універсальні дані потенційно притягують до відповідальності як уряди, так і громадян. Коротше кажучи, Брін був оптимістом і наполягав на тому, що ми не так вже й далеко від радикально покращеного суспільства. Він наполягав на тому, що більше інформації звідусіль може сприяти більшій цивілі-

зованості й навіть перерозподілу влади. У такому майбутньому не матиме значення, що держава вимагає прозорості від своїх громадян, доки держава пропонує прозорість у відповідь [53]. Чи стане Прозоре суспільство Бріна врешті-решт реальністю, чи ми зіткнемося з чимось більш похмурим? Брюс Шнайєер, авторитетний експерт з кібербезпеки, який свого часу очолював службу безпеки British Telecom, скептично відповів на це запитання, наполягаючи на тому, що право власності на ці дані навряд чи буде достатнім для того, щоб сприяти колективній людській підзвітності, яку передбачає Брін [54; 55]. Який би оракул не виявився правим, майбутнє стрімко наближається, і коли воно настане, наші нинішні системи управління інтернетом і кіберстійкості навряд чи зможуть з ним впоратися.

Людські помилки та застарілі системи в кіберфізичних екосистемах. У 2030 році інтернет речей проникне у значну частину транспортної, енергетичної, водопровідної та промислової інфраструктури, щоб підвищити ефективність та покращити прийняття інтелектуальних рішень. Крім того, відбудеться значне збільшення кількості розумних пристроїв, які пересічний користувач пов'язує з собою (станом на 2021 рік середньостатистична людина мала сім розумних пристроїв) [56]. Через це може стати надзвичайно складно обслуговувати всі пристрої та керувати ними, особливо з точки зору безпеки. Крім того, виробники смарт-пристроїв, ймовірно, не зможуть навчити кінцевих користувачів необхідності обслуговування пристроїв. Швидке впровадження IoT і постійний дефіцит навичок призведе до того, що до 2030 року бракуватиме знань, підготовки й розуміння кіберфізичної екосистеми, що призведе до проблем з підтримкою безпеки IT, пов'язаних з неправильною конфігурацією, несвоєчасним обслуговуванням і неадекватною підтримкою в кінці терміну служби застарілого програмного забезпечення IoT [24]. На додаток до цих проблем, зловмисники можуть розгортати інтелектуальні атаки з використанням таких методів, як генеративні ворожі мережі (Generative Adversarial Networks, GAN), які можуть різко знизити рівень виявлення кібератак. Одним із прикладів використання GAN може бути атака на сервери, що розповсюджують патчі, з метою зриву запланованих оновлень [57]. Через критичність пристроїв, це може створити системний ризик, що призводить до перебоїв у роботі, пошкоджень, а також перехоплення даних між пристроями.

На стороні кінцевого користувача пристроями «інтернету речей» часто керують мобільні пристрої, що працюють на iOS або Android. Кінцеві користувачі спілкуються через свої мобільні додатки з розумними пристроями, які є частиною їхнього будинку, транспорту або іншого оточення. Зловмисники можуть спробувати отримати початковий доступ до мобільних пристроїв за допомогою підробки біометричних даних, атак грубої сили або використання вразливостей на пристрої. Отримавши доступ до телефона й законних каналів зв'язку між телефоном кінцевого користувача та інфраструктурою, вони можуть втручатися в роботу смарт-пристроїв, проникати в мережу або отримати доступ до облікового запису, який керує смарт-пристроями [58]. У промисловій екосистемі зловмисники можуть отримати початковий доступ через співробітників за допомогою атаки соціальної інженерії або через їхні кінцеві точки, переміститься вглиб корпоративної мережі й шукати пристрої з доступом до інтернету, які підключені до промислових систем управління. Крім того, атаки можуть бути успішними через тимчасові кібер-активи, які розгортаються з незахищеною конфігурацією, в тому числі від сторонніх постачальників і партнерів

Цілеспрямовані атаки (наприклад, програми-вимагачі), посилені даними зі смарт-пристроїв. У 2030 році збір поведінкових даних збільшиться в геометричній прогресії. Використання смарт-пристроїв у нашому повсякденному житті значно зросте; будуть збиратися дані з усіх аспектів життя, що призведе до створення точного та унікального поведінкового профілю кожного користувача. Зібрані дані можуть включати (серед інших джерел) дані про стан здоров'я з натільних пристроїв і медичного обладнання або з пристроїв інтернету речей в «розумних будинках», які збирають інформацію про поведінку вдома, дані про пересування або поведінку на онлайн-платформах. Оскільки смарт-пристрої часто будуть незахищеними через громіздкість пристроїв і недостатню обізнаність кінцевих користувачів ці дані можуть бути використані [50]. Інтелектуальні периферійні пристрої вже зараз важко захистити від маніпуляцій та прослуховування.

Злочинні групи намагатимуться отримати доступ до величезних масивів даних, щоб адаптувати атаки соціальної інженерії на основі поведінкового профілю користувача. Рівень витонченості цих атак соціальної інженерії змусить кінцевих користувачів, правоохоронні органи та уряди шукати нові способи запобігання соціальній інженерії та покращення автентифікації.

Зловмисники можуть отримати початковий доступ через підключені до інтернету смарт-пристрої, які не мають оновлень або все ще працюють зі стандартними налаштуваннями. Злочинці та хакери-найманці [44] збиратимуть інформацію про особу жертви, облікові дані та контактну інформацію, щоб отримати початковий доступ, а потім просуватимуться далі в мережі, щоб отримати доступ до більш чутливої інформації. Зловмисники використовуватимуть автоматизований збір даних і проникнення, зіставлятимуть та інтерпретуватимуть дані для створення поведінкового профілю своєї жертви. Щоб утримати свої позиції, зловмисники використовуватимуть методи наполегливості

[24]. За допомогою поведінкового профілю вони намагатимуться отримати доступ до фінансових активів, використовуватимуть профіль для підміни високопосадових осіб у мережі жертви або продаватимуть зібрані дані на чорному ринку.

Брак аналізу та контролю космічної інфраструктури та об'єктів. Початок 2010-х і 2020-х років розпочав нову еру космічних подорожей, коли приватні компанії приєдналися до урядів у прагненні досліджувати наш всесвіт. До 2030 року космічний сектор, ймовірно, трансформується ще більше завдяки збільшенню інвестицій приватних суб'єктів, партнерствам між приватними компаніями та урядами, а також зростанню геополітичної та комерційної конкуренції в космосі [24].

Швидке зростання цього сектору уможливить надання багатьох ключових послуг. Незважаючи на прогрес, досягнутий за останні роки, цей сектор все ще залишається в центрі уваги безпекової спільноти.

З точки зору безпеки бракує розуміння, аналізу й контролю космічної інфраструктури. Без ширшого загальноєвропейського фокусу розбудова надійного захисту космічної інфраструктури може бути надто повільною (наприклад, науково-дослідні проекти, які потребують часу на планування й бюджетування). Це також означає, що може бракувати своєчасної підготовки до ідентифікації та використання невідомих вразливостей [59] (нульові дні) – якщо ресурси не розподілені належним чином. Ринки стимулюють приватні компанії швидше впроваджувати інновації та знижувати витрати за рахунок кібербезпеки. Приватні компанії можуть спробувати використати це для саботажу своїх конкурентів; уряди можуть спробувати використати вразливості для створення конкурентної геополітичної переваги в космосі; а злочинні угруповання використовуватимуть вразливості, щоб вимагати у компаній фінансову вигоду і створювати хаос [24].

Через перетин приватної та державної інфраструктури в космосі зловмисники можуть отримати початковий доступ до космічної інфраструктури, обравши своєю мішенню приватних суб'єктів, урядові установи або окремих осіб, які взаємодіють з інфраструктурою. Оскільки уряди й суспільства значною мірою залежать від супутників (наприклад, GPS), державні зловмисники й хакери-найманці намагатимуться отримати початковий доступ до апаратного забезпечення через атаки на ланцюжки поставок і використовуватимуть методи, щоб зберегти свою присутність у космічній інфраструктурі, зокрема на базових станціях [24]. Зловмисники використовуватимуть наявні технології, щоб обійти механізми захисту й виявлення, але залишатимуться бездіяльними, доки не використають їх у стратегічних цілях, наприклад, під час конфлікту як засіб гібридної війни. Впровадження зброї космічного базування може змінити геополітичну парадигму.

Зростання сучасних гібридних загроз. До 2030 року кібератаки стануть більш витонченими й будуть поєднуватися з фізичними або офлайн-атаками. Методи атак постійно розвиваються і часто комбінуються – послідовно й паралельно – для досягнення своїх цілей. Ці гібридні операції складніше виявити й захиститися від них через їхню складність і тенденцію розглядати кожну атаку окремо [24]. За нового способу дій інструменти виявлення потребують більшої кореляційної здатності, в тому числі пов'язувати, здавалося б, не пов'язані між собою події. Тому вони становлять все більший виклик як для урядів, так і для компаній та громадян. У минулому гібридні атаки здійснювалися переважно державними суб'єктами як поєднання традиційних і кібервійськ. У 2030 році гібридні загрози еволюціонували до застосування нових технологій та комбінування різних типів механізмів експлуатації для того, щоб обійти існуючі системи реагування [24].

Наприклад, зловмисники все частіше використовуватимуть штучний інтелект і глибоке навчання, щоб об'єднати свої можливості [49] для створення нових, непередбачуваних способів дій. Зловмисники використовуватимуть одночасну комбінацію методів для отримання початкового доступу, включаючи збір великих даних для адаптації своїх фішингових кампаній, машинне навчання для інтерпретації даних, розробку нових інструментів для обходу захисних механізмів і поєднання фізичного й віртуального для здійснення своїх атак. Зі збільшенням кількості смарт-пристроїв, використання хмарних технологій, збільшенням кількості онлайн-ідентифікаторів і соціальних платформ, а також цифрових посвідчень особи, виданих урядами, зловмисники отримають безліч нових сфер для використання й комбінування для створення креативних векторів атак.

Дефіцит навичок. До 2030 року проблема дефіциту навичок [60] не буде вирішена. Хоча зростання кількості незаповнених робочих місць у сфері кібербезпеки вирівнялося, дефіцит навичок і надалі становитиме значний ризик для суспільства та урядів. Одним з важливих факторів, який впливатиме на загрозу у 2030 році, є готовність (і ресурси) організацій розширювати штат і розвивати таланти. Впровадження функцій кібербезпеки також постраждає через брак навичок і загальної зрілості функцій кібербезпеки, навіть за наявності бажання.

У міру того, як технології все більше інтегруються в наше життя, пересічні громадяни можуть стати апатичними – всі їхні комунікації та дії управляються десь іззовні, і вони не мають на це жодного впливу. Цей ризик посилюватиметься взаємодією між новими технологіями та застарі-

лими технологіями, для яких робоча сила не була підготовлена – знання застарілих технологій передаються недостатньо швидко, щоб управляти цим ризиком у 2030 році [24]. На додаток до дефіциту застарілих навичок, нові технології, такі як розумні пристрої, штучний інтелект, космічна інфраструктура або квантові обчислення, створюватимуть нові виклики кібербезпеці. Злочинні групи обиратимуть організації, установи та компанії, які мають велику кількість незаповнених вакансій у сфері кібербезпеки, з метою пошуку вразливостей та використання цих вразливостей для отримання фінансової вигоди.

Зловмисники аналізують організаційні навички та недоліки, щоб отримати уявлення про слабкі місця в захисті, потенційні вразливості та можливості для використання їхніх систем і мереж. Публічні оголошення про вакансії часто містять детальну інформацію про те, яких навичок наразі бракує в компанії чи державній установі, що дає зловмисникам уявлення про можливі вектори проникнення. Крім того, зловмисники намагатимуться отримати інформацію з відкритих і закритих джерел, щоб зібрати організаційну та мережеву інформацію і виявити застарілі системи з відомими вразливостями. Наприклад, в оголошенні про вакансію на місцевій електростанції може бути вказаний постачальник і тип продукту, для якого їм потрібна підтримка – це дає зловмисникам достатньо часу для дослідження вразливостей конкретного продукту. Крім того, розробляючи нові технології, працівники, які мають кваліфікацію для впровадження безпеки, не мають достатньої пропускної здатності, щоб застосувати безпеку до виходу на ринок через брак кваліфікованих працівників.

Транскордонні постачальники послуг ІКТ як єдина точка відмови. У 2030 році технологічна взаємопов'язаність буде посилюватися. Межа між фізичним і кіберпростором ще більше розмиватиметься, оскільки такі сектори інфраструктури, як транспорт, охорона здоров'я, електромережі та промисловість [50], все більше покладаються на постачальників послуг ІКТ для підключення до інтернету та управління всіма міжпристрійними зв'язками. Хоча їхня відповідальність за підтримку функціонування суспільства була значною ще у 2022 році, до 2030 року їхня важливість зростає ще більше. Провайдери ІКТ-послуг та їхня інфраструктура, включаючи супутникові технології, є основою суспільства і тому можуть стати єдиною точкою відмови. Розумні міста є прикладом того, що через 10 років операційні мережі стануть ще більш критично важливими. Отже, ці постачальники послуг, імовірно, стануть мішенню для урядів, терористів і злочинних угруповань. Використання вразливостей для отримання доступу до їхніх мереж, кінцевих точок, центрів обробки даних або інших фізичних компонентів ІКТ-інфраструктури може завдати шкоди містам і цілим регіонам [24].

Іноземні уряди можуть спробувати використати це для дестабілізації країн, терористи – для нагнітання страху й досягнення політичних цілей, а злочинні угруповання – для захоплення міст у заручники. ІКТ-інфраструктура [61], ймовірно, буде використана як зброя під час майбутнього конфлікту. Провайдерам ІКТ доведеться захищатися від спонсорованих державою, наполегливих і високорозвинених атак, які спираються на дані урядових розвідувальних служб і наступальні кіберпотужності. Ресурси, які будуть виділені для такої атаки, є значними – зловмисникам знадобиться час, щоб уникнути традиційних функцій реагування, і вони, імовірно, розгорнуть гібридні атаки для отримання початкового доступу й нещодавно розроблених експлойтів з можливостями командування та контролю. Оскільки сектор ІКТ з'єднує так багато критично важливих послуг, він стане мішенню для таких технологій, як бекдори, фізичні маніпуляції й відмова в обслуговуванні, через масштаб збитків, яких можна досягти.

Зловживання штучним інтелектом. ШІ можна маніпулювати з моменту його створення та протягом усього життєвого циклу за допомогою маніпуляцій з навчанням і ворожих атак [62]. Несвідома упередженість ШІ була добре відома на початку 20-х років, однак у 2030 році існує реальна загроза навмисного маніпулювання алгоритмами ШІ та навчальними даними. Так само будь-яке спотворене навчання алгоритмів ШІ може навчити їх приймати неправильні рішення щодо секторів підвищеного ризику [63].

Зловмисники намагатимуться використати можливості додатків зі штучним інтелектом для формування результатів прийняття рішень і збору інформації про потенційних жертв. Наприклад, вони можуть втручатися в навчальні набори даних для створення дисфункціональних і шкідливих програм штучного інтелекту – це може стосуватися й проектів збору даних на основі краудсорсингу (crowdsourcing). Крім того, зловмисники можуть використовувати ШІ в наступальних або злочинних цілях – наприклад, аналізувати поведінку користувачів для створення високорозвинених фішингових або гібридних кампаній [24].

ШІ може бути використаний для посилення багатьох нечесних дій, таких як створення дезінформації та фейкового контенту, використання упереджень, збір біометричних та інших конфіденційних даних, створення військових роботів, отруєння даних тощо.

Майбутнє кіберстійкості частково пов'язане з людьми як антидотом до вразливостей інтернету. Однак у той час як нова логіка безпеки систем передбачає необхідність різноманітності та навіть,

можливо, обережного відокремлення, загальна тенденція в інформаційних технологіях полягає в конвергенції людей і комп'ютерів. Мабуть, найпомітнішим проявом цього є світ ігор, де ми спостерігаємо прагнення об'єднати людину й машину в симульованій топографії [64]. Витончені ігри все частіше використовуються провайдерами військової підготовки для створення різноманітних тренувальних середовищ. Як у військових, так і в розважальних цілях, реальність і кіберпростір дедалі більше зближуються, і наступним викликом є безперешкодна взаємодія між мозком і комп'ютером.

Найпоширеніший досвід цього можна знайти в сучасних ігрових технологіях, які використовують розпізнавання зображень для перетворення людських жестів на команди. Система Microsoft Xbox Kinect дозволяє гравцям взаємодіяти з грою через фізичні рухи, зафіксовані відеокамерою. Очевидно, що Xbox вимагає фізичного руху. Однак у 2009 році компанія Mattel випустила «Mindflex» - гру, яка отримувала вхідні дані безпосередньо від мозку. Вхідні дані були відносно примітивними, оскільки гравець не міг свідомо керувати пристроєм. Замість цього гра зчитувала електромагнітні імпульси (EMI). У лабораторних умовах піддослідних навчили набирати номер мобільного телефону, використовуючи лише EMI. Всі ці пристрої, хоч і примітивні, тим не менш, вказують шлях до майбутнього технологій і потенціалу, який пропонує інтерфейс між комп'ютером і мозком [1].

Очевидним застосуванням зростаючого зв'язку між людьми та інтернетом є превентивна охорона здоров'я. Вчені-медики все більше цікавляться маленькими чіпами, які відстежують життєво важливі показники й можуть вказати на ранній початок проблем з серцем, інсультів та інших захворювань [65; 66]. Рання діагностика та втручання до того, як ці захворювання настануть, суттєво підвищує шанси на успішний результат. Ця технологія вже існує. Використовуючи нові технології, наприклад, смартфони з підтримкою GPS, ми можемо вимірювати ключові життєві показники, скільки часу ми спимо, куди їдемо, що їмо й п'ємо та як проводимо свій день. Зібравши ці дані, одержимі самоспостереженням люди розміщують їх у «хмарі». Останнім прикладом є «Fitbit» - крихітний пристрій, який можна прикріпити до одягу та який бездротовим способом надсилає медичні дані на веб-сайт, що створює графіки активності суб'єкта [1].

Найважливіші зміни відбулися в медичній технології, призначеній для лікування військових поранених. Вищі показники виживання на полях битв в Іраку та Афганістані в поєднанні з травмами, що змінюють життя, спричиненими саморобними вибуховими пристроями, підвищили попит на більш складні протези кінцівок. Виклик полягав у тому, щоб з'єднати сучасні протези з нервовою системою, щоб досягти чогось набагато ближчого до природного контролю з боку пацієнта. За останні п'ять років відбулися радикальні зміни у можливості підключення мікроелектроніки до нервової системи людини. Результати були вражаючими. Дрібна моторика, яку забезпечують ці пристрої, майже не відрізняється від тієї, яку забезпечують справжні кінцівки. Вчені очікують, що це дослідження призведе до створення нейронних протезів для всього тіла, спрямованих на відновлення повних, життєво важливих функцій руху паралізованих пацієнтів [1]. Коротше кажучи, проблема поєднання електронних повідомлень, що надсилаються людським мозком, і мікроелектронних систем буде вирішена в найближчі 10 років [67].

Мало хто з учених сумнівається, що прямий інтерфейс між комп'ютером і мозком не за горами. Якими можуть бути наслідки для кіберпростору? Такий розвиток матиме значні економічні, соціальні та політичні наслідки. Люди, які будуть постійно підключені до інтернету в більш фундаментальний спосіб, стануть більш здібними – але також будуть думати й діяти по-іншому. Можливість бути підключеним, а отже, бути на «постійному зв'язку» буде одним з найбільш фундаментальних рішень, які чекають на людину в середині двадцять першого століття [1].

> *Виникає запитання: як досягти кіберстійкості у світі, в якому людина все більше стає синонімом інтернету?*

Ця можливість викликає альтернативні бачення, утопічні або антиутопічні. Можливо, зростаючий зв'язок між 8 мільярдами людей та інтернетом нарешті створить кіберпростір, який дійсно представлятиме глобальне надбання – спільну віртуальну топографію, засновану на взаємній власності, повазі й довірі. З іншого боку, це нове середовище може призвести до збільшення глобальних ризиків і невизначеності [1].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Lewis, Herrington & Richard, Aldrich (2013). The Future of Cyber-Resilience in an Age of Global Complexity. POLITICS, 33 (4), 299–310. DOI: 10.1111/1467-9256.12035
2. Ministry of Defence (1976). Working Group on Testing of Computer Security, 1976/7 (D/DCCIS/56/8/5/4), DEFE68/287, TNA.
3. Warner, M. (2012). Cybersecurity: A Pre-historyю. Intelligence and National Security, 27(5), 781–799.
4. Arquilla, J. & Ronfeldt, D. (1993). Cyberwar is Coming! RAND Corporation RP-223.
5. Rid, T. (2012). Cyber War Will Not Take Place. Journal of Strategic Studies, 35 (1), 5–32.

6. Deibert, R.J., Rohozinski, R. & Crete-Nishihata, M. (2012). Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War. Security Dialogue, 43 (1), 3–24.
7. Farwell, J.P. & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. Survival, 53 (1), 23–40.
8. Американский адмирал подтвердил, что Россия ведет кибервойну против Украины. URL: https://web.archive.org/web/20160429082331/http://ain.ua/2014/03/17/515999
9. Russian Electronic Warfare in Ukraine: Between Real and Imaginable - Jamestown. Jamestown. Retrieved from https://jamestown.org/program/russian-electronic-warfare-ukraine-real-imaginable/
10. Російські хакери у 2023 році збільшили кількість атак на Україну: що відомо. URL: unian.ua/war/rosiyski-hakeri-u-2023-roci-zbilshili-kilkist-atak-na-ukrajinu-shcho-vidomo-12426765.html?_gl=1*b62dke*_ga*NTUzMzI0Mzg3LjE2OTc0NzgxNzY.*_ga_TECJ2YKWSJ*MTY5NzQ3ODE3NS4xLjAuMTY5NzQ3ODE4MC41NS4wLjA.*_ga_DENC12J6P3*MTY5NzQ3ODE3NS4xLjAuMTY5NzQ3ODE3OS41Ni4wLjA.
11. Statement from the Press Secretary. The White House. Retrieved from https://uk.wikipedia.org/wiki/%D0%A0%D0%BE%D1%81%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%BE-%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%81%D1%8C%D0%BA%D0%B0_%D0%B2%D1%96%D0%B9%D0%BD%D0%B0_(%D0%B7_2014)
12. Атака на «Киевстар». Прекратил работать крупнейший в Украине оператор мобильной связи, СБУ подозревает Россию. URL: https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0_%D0%BD%D0%B0_%C2%AB%D0%9A%D0%B8%D1%97%D0%B2%D1%81%D1%82%D0%B0%D1%80%C2%BB_(2023)
13. НБУ рекомендує банкам створити резервні канали зв'язку після кібератаки на «Київстар». РБК-Україна. URL: https://www.rbc.ua/rus/news/nbu-rekomendue-bankam-stvoriti-rezervni-kanali-1702538362.html
14. «Київстар» не працює. Що сталось і чи можна обійти проблему. BBC News Ukrainian (укр.). URL: https://www.bbc.com/ukrainian/articles/cz92xrkklwro
15. Espiner, T. (2011). Cybercrime Cost Estimate is «Sales Exercise». Say Experts', Znet, 18 February. Retrieved from http://www.zdnet.com/cybercrime-cost-estimate-is-sales-exercise-say-experts-3040091866/
16. Curtis, S. (2011). Government Cyber Crime Report Debunked, Tecweek Europe, 22 February.
17. Press, L. (2011). The State of the Internet in Cuba. Unpublished research paper. Retrieved from som.csudh.edu/fac/lpress/cuba/chapters/lpdraft2.docx?.
18. Zhang, D.J. (2010). Integrating Cyber Security into Nuclear Digital I&C Safety Systems. ASME Conference Proceedings 18th International Conference on Nuclear Engineering, Vol. 1/Instrumentation and Controls (ICONE18).
19. Stolfo, S.J. (ed.) (2008). Insider Attack and Cyber Security: Beyond the Hacker. Boston, MA: Springer.
20. Arce, I. (2003). The Weakest Link Revisited. IEEE Security and Privacy, 1 (2), 72–76.
21. Dornhege, G., Millan, J., Hinterberger, T., McFarland, D. & Müller, K. (2007). Toward Brain–Computer Interfacing. Cambridge, MA: MIT Press.
22. Bures, O. (2006). EU Counterterrorism Policy: A Paper Tiger? Terrorism and Political. Violence, 18 (1), 57–78.
23. European Foresight Platform (efp), What is Foresight? (2010). Retrieved from http://www.foresight-platform.eu/community/forlearn/what-is-foresight/
24. Foresight Challenges. A study to enable foresight on emerging and future cybersecurity challenges. European Union Agency for Cybersecurity (ENISA), 2021.
25. Haegeman, K., Spiesberger, M. & Könnölä, T. (2017). Evaluating foresight in transitional research programming. Technological Forecasting and Social Change, 115, 313 – 326.
26. Althonayan, Abraham & Alina Andronache (2019). Resiliency under strategic foresight: The effects of cybersecurity management and enterprise risk management alignment. 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA). IEEE.
27. Senge, Peter M. (1990). The fifth discipline: the art and practice of the learning organization. New York: Doubleday/Currency
28. Jackck, E. Smith & Saritas, Ozcan (2011). Science and technology foresight baker's dozen: A pocket primer of comparative and combined foresight methods. Foresight, 13 (2), 79-96.
29. Megatrend / Trend / Driver / Issue, 2010. Retrieved from http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/analysis/megatrend-trend-driver-issue/
30. GCPSE, Foresight (2014). The Manual, UNDP Global Centre for Public Service Excellence, Singapore.
31. NISTEP. Retrieved from https://www.nistep.go.jp/en/?page_id=56
32. A Refresher on Regression Analysis. Retrieved from https://hbr.org/2015/11/a-refresher-on-regression-analysis
33. Jackson, M. (2013). Practical Foresight Guide– Chapter 1.
34. Vanatta, N. & Johnson, B.D. (2019). Threatcasting: a framework and process to model future operating environment. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 16 (1), 79 – 88.
35. Matthew, Rosenquist & Timothy, Casey (2009). Prioritizing Information Security Risks with Threat Agent Risk Assessment. Intel Information Technology, USA, 1-8.
36. Note that Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University. Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13473
37. Barber, C. (2020). Cyber Security Predicting the Future.
38. POLI.design and Oblo, Service Design Tools, Tools. Retrieved from https://servicedesigntools.org/tools

39. Futures platform. Retrieved from https://www.futuresplatform.com/product
40. IFTF - The Future Is Wide Open. Retrieved from https://www.iftf.org/uploads/media/GovFuturesLab_Toolkit.pdf
41. Teach the Future: Futures Thinking Educators. Retrieved from https://www.teachthefuture.org/
42. Kayser, Victoria & Knut Blind (2017). Extending the knowledge base of foresight: The contribution of text mining. Technological Forecasting and Social Change, 116, 208-215.
43. ENISA (2022). Identifying Emerging Cyber Security Threats and Challenges for 2030.
44. ENISA (2022). Threat Landscape Report. Retrieved from https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_de.pdf
45. ENISA (2016). Threat Taxonomy. Retrieved from https://www.enisa.europa.eu/topics/threatrisk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy
46. ENISA (2021, July). Understanding the increase in Supply Chain Security Attacks. Retrieved from https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-insupply-chain-security-attacks
47. Jubb, S. (2022, August). Escalating supply chain cyber-attacks need a strategic response. Retrieved from https://www.openaccessgovernment.org/escalating-supply-chain-cyberattacks-need-a rategicresponse/141371/#:~:text=What%20are%20supply%20chain%20attacks,and%20cause%20disruptions%20or%20outages
48. Newman, L. H. (2021, December). A Year After the SolarWinds Hack, Supply Chain Threats. Retrieved from https://glock.co.uk/blog/a-year-after-the-solarwinds-hack-supply-chain-threats-still-loom-wired/?doing_wp_cron=1706623406.9687340259552001953125
49. Shein, E. (2022, August). Deepfake attacks and cyber extortion are creating mounting risks. Retrieved from https://www.techrepublic.com/article/deepfake-attacks-and-cyberextortion-are-creating-mounting-risks/
50. ENISA (2021). Threat Landscape. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
51. ENISA (2020). Personal Data Breaches. Retrieved from https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches
52. ENISA (2021). Retrieved from Foresight Challenges: https://www.enisa.europa.eu/publications/foresight-challenges
53. Brin, D. (1998). The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom? Reading, MA: Addison-Wesley.
54. Brin, D. (2008). David Brin Rebuts Schneier in Defense of a Transparent Society. Wired News, 12 March.
55. Schneier, B. (2008). The Myth of the «Transparent Society». Wired News, 6 March. Retrieved from http://bakerinstitute.org/publications/ITP-pub-PlanksOfUSInternationalCyberPolicy-052112.pdf
56. BSI-Magazin (2021, January). Mit Sicherheit. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSIMagazin_2021_01.pdf?__blob=publicationFile&v=4
57. Shi, A. (2021, September). Cyber Attacks Detection Based on Generative Adversarial Networks. Retrieved from https://ieeexplore.ieee.org/document/9681469
58. SOCRadar (2022, May). Common IoT Attacks that Compromise Security. Retrieved from https://socradar.io/common-iot-attacks-that-compromisesecurity/#:~:text=Privilege%20escalation%3A%20Attackers%20could%20exploit,unauthorized%20access%20 to%20the%20network.
59. Erwin, S. (2022, March). Cyber warfare gets real for satellite operators. Retrieved from https://spacenews.com/cyber-warfare-gets-real-for-satellite-operators/
60. Fortinet (2022). Retrieved from fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf
61. Allianz (2016). Cyber attacks on critical infrastructure. Retrieved from https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-oncritical-infrastructure.html
62. West, T. (2017). The Future of Weaponized Artificial Intelligence. Retrieved from https://threatcasting.asu.edu/sites/default/files/2019-12/ThreatcastingWest2017.pdf
63. Commission, E. (2022). Regulatory framework proposal on artificial intelligence. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
64. Der Derian, J. (1990). The (S)pace of International Relations: Simulation, Surveillance, and Speed, International Studies Quarterly, 34 (3), 295–310.
65. Michael, K. & Michael, M.G. (2005). Microchipping People: The Rise of the Electrophorus. Quadrant, 49(3), 22–33.
66. Streitfield, D. (2002). First Humans to Receive ID Chips; Technology: Device Injected under the Skin Will Provide Identification and Medical Information. Los Angeles Times, 9 May.
67. Lebedev, M.A. & Nicolelis, M.A. (2006). Brain–Machine Interfaces: Past, Present and Future. Trends in Neuroscience, 29(9), 536–546.

DOI: https://doi.org/10.36486/978-966-2310-66-5-27

Знання деяких принципів легко заміщує незнання
Клод-Адріан Гельвецій

РОЗДІЛ 27
Аналіз соціальних мереж

Олександр Засць

Соціальні мережі є сильним засобом комунікації мільйонів людей. Під соціальною мережею розуміється безліч об'єктів, які можуть вступати у взаємодію один з одним. З формальної точки зору такі мережі зручно представляти у графічному вигляді та застосовувати до них аналітичні моделі. [1, с. 4]

Соціальна мережа на сьогоднішній день є ідеальним місцем для отримання інформації про людей. За різними даними та критеріями можна отримати велику кількість інформації, яка буде корисною для правоохоронних органів.

> *Аналіз соціальних мереж (англ. Social Network Analysis) – це дослідження соціальних мереж, що розглядає соціальні відносини в термінах теорії мереж.*

Ці терміни включають поняття вузла (відображає окремого учасника в межах мережі) і зв'язку (відображає такі відносини між індивідами, як дружба, спорідненість, становище в організації, інтимні відносини тощо). Ці мережі часто описуються як соціально-мережеві схеми, де вузли представлені як крапки, а зв'язки представлені як лінії [2, с. 68, с. 165].

У рамках теорії складних мереж вивчаються мережеві характеристики не лише з точки зору топології мереж, але і статистичні феномени, ваговий розподіл окремих вузлів і ребер, ефекти протікання і провідності. Попри те, що до предмету теорії складних мереж потрапляють різні мережі (електричні, транспортні, інформаційні), найбільший внесок у розвиток цієї теорії внесли дослідження саме соціальних мереж.

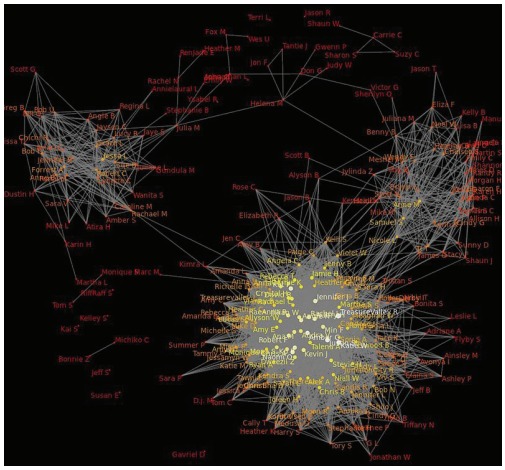


Рисунок 27.1. Приклад крапок, вершин та зв'язків між ними

У теорії складних мереж виділяють три основні напрями:

- *дослідження статистичних властивостей, які характеризують поведінку мереж;*
- *створення моделей мереж;*
- *прогнозування поведінки мереж при зміні структурних властивостей.*

Аналіз джерела даних може призвести до виявлення різних артефактів, таких як повідомлення, листи, дзвінки, зображення, текстові документи, відео, дані реєстру тощо. Серед них можна знайти список контактів, отриманих, наприклад, з історії миттєвих повідомлень.

Контакт – інформація, що характеризує людину чи групу осіб. Контакт може бути отриманий з таких джерел: дзвінки; голосові повідомлення; короткі текстові повідомлення; миттєві повідомлення; електронні листи; адресна книга мобільного телефону; інформації про аналізований пристрій. Відповідно, контакт може містити назву облікового запису, псевдонім, адресу електронної пошти, телефонні номери, ім'я, прізвище, назву компанії тощо. Наприклад, з електронного листа витягуються контакти відправника, одержувачів, одержувачів копії листа та прихованих одержувачів копії листа.

Взаємодія – це факт передачі данних між контактами. Наприклад, дзвінок, голосове повідомлення, коротке текстове повідомлення, миттєве повідомлення або електронний лист. У деяких контактів може бути взаємодія з іншими контактам, якщо вони, наприклад, отримані з адресної книжки мобільного телефону. Також зауважимо, що взаємодії існують лише між контактами одного типу. Наприклад, вилучені дані не надають інформації про взаємодії між контактом, отриманим з електронного листа, та контактом з історії голосових повідомлень.

Аналітик може припустити, що пара контактів належить одній й тій самій людині, отже існує взаємодія для людей, представленими контактами різних типів, але напевно стверджувати цього не можна.

Для автоматизації аналізу соціальних зв'язків необхідно заздалегідь знаходити і об'єднувати контакти, що належать тим самим особам. Таким чином аналітик зможе аналізувати не окремі повідомлення та дзвінки, а соціальні взаємодії між людьми загалом.

Сутність – людина чи група осіб, представлені ідентифікуючими даними: назва облікового запису; адреса електронної пошти; номер телефону; прізвище; ім'я; псевдонім тощо. Між сутностями, як об'єднаннями контактів, може бути взаємодія. Між двома сутностями існує зв'язок, якщо відбувся хоча б один факт взаємодії між ними. Кожний зв'язок має вагу, що характеризує його значимість. [3, с. 29] Значення ваги залежить від типу, кількості та часу взаємодій. Нижче вказані взаємодії в порядку зменшення значимості:

- *дзвінок;*
- *голосове повідомлення;*
- *коротке текстове повідомлення;*
- *миттєве повідомлення;*
- *електронний лист.*

Наприклад, дзвінок вважається більш значним типом взаємодії, ніж електронний лист. Використання телефону передбачає спілкування тет-а-тет і велику залученість до діалогу, тоді як у листа можуть бути кілька одержувачів, і відповідь на нього може прийти через кілька годин чи навіть днів.

Кількість взаємодій також свідчить про ступінь близькості між людьми. Так зв'язки з найбільшою кількістю взаємодій найчастіше вказують на родичів, близьких друзів чи обговорення якоїсь спільної справи.

Крім контактів, що належать реальним людям, існують електронні адреси компаній, що розсилають рекламні пропозиції або новини, спам-боти тощо. Вони зазвичай надсилають безліч листів або повідомлень за короткий часовий проміжок, але це не значить, що вони мають високу цінність. Тому для оцінки значущості варто враховувати час взаємодії між сутностями.

Класифікація зв'язків

Гомогенність (англ. Homophily): ступінь, з якою подібні учасники формують зв'язок між собою. Схожість може бути визначена за статевою ознакою, расою, віком, родом занять, досягненнями в галузі навчання, статусом, цінностями або за іншими характеристиками, що виділяються.

Множинність (англ. Multiplexity): кількість форм у зв'язку. Наприклад, дві людини, які є друзями та працюють разом матимуть множинність, рівну 2. Множинність пов'язана з міцністю відносин.

Взаємність (англ. Mutuality / Reciprocity): ступінь, з якою двоє учасників відповідають один одному взаємністю у сфері дружніх чи інших взаємодій.

Закритість мережі (англ. Network Closure): міра повноти реляційних тріад. Присвоєння індивідам ступеня закритості мережі (тобто те, що й друзі також є друзями між собою) називається транзитивністю. Транзитивність є наслідком індивідуальної чи ситуаційної особливості, що полягає у потребі когнітивної закритості.

Сусідство (англ. Propinquity): схильність учасників мати більше зв'язків із тими, хто знаходиться ближче з погляду географії.

Міст (англ. Bridge): індивід, чиї слабкі зв'язки заповнюють структурні прогалини, забезпечуючи єдине з'єднання між двома індивідами чи кластерами. Він також включає найкоротший шлях, коли більш довгий шлях неможливий через високий ризик спотворення повідомлення або неможливості доставки.

Центральність (англ. Centrality): центральність відноситься до групи метрик, метою яких є визначення «значущості» або «впливу» (у різних значеннях) певного вузла (або групи) у мережі. Прикладами загальних методів вимірювання «центральності» є визначення центральності за посередництвом, центральності близькості, центральності власного вектора, альфа центральності та центральності за ступенем.

Щільність – відношення прямих зв'язків у мережі до загальної кількості зв'язків.

Відстань (англ. Distance): мінімальна кількість зв'язків, необхідна для з'єднання двох певних учасників.

Структурні прогалини (Structural holes): відсутність зв'язків між двома частинами мережі. Пошук та використання структурної прогалини може дати конкурентну перевагу. Ця концепція була розроблена соціологом Рональдом Бертом.

Сила зв'язку (англ. Tie Strength): визначається лінійною комбінацією часу, емоційної інтенсивності, близькості та взаємності. Сильні зв'язки визначаються гомогенністю, спорідненістю та транзитивністю, тоді як слабкі – мостами.

Група окреслюється «клікою» - група людей, політичне угруповання, об'єднані спільними недобрими, зокрема корисливими цілями, якщо кожен індивід у ній безпосередньо пов'язаний з іншим індивідом. Група визначається як «коло спілкування», якщо в ній менше вимог до прямого контакту, який може бути не визначений.

Коефіцієнт кластеризації: міра ймовірності, з якою два партнери одного вузла є приятелями. Високий коефіцієнт кластеризації відповідає значній вирогідності «злочинного оточення». Рівень «центральних» фігурантів передбачає їх порівняння в рамках мережі. «Кліка» - підгрупа, що характеризуються інтенсивнішим внутрішнім обміном. Структурний мережевий рівень визначається домінуванням і зв'язаністю. Домінування - це відхилення від рівномірного розподілу зв'язків між «центрами» і «кліками». В системі, яка характеризується високим ступенем домінування, більшість зв'язків будуть з'єднувати «центри» і «кліки».

Згуртованість: ступінь, з яким учасники пов'язані безпосередньо один з одним за допомогою соціальних зв'язків [4].

Візуальне уявлення соціальних мереж важливо для розуміння даних мережі та передачі результатів аналізу. Найчастіше аналітичне програмне забезпечення має модулі для візуалізації мережі. Дослідження даних здійснюється шляхом відображення вузлів та зв'язків у різних шарах, а також присвоювання вузлам кольорів, розмірів та інших додаткових властивостей. Візуальне подання мереж може виступати як потужний метод передачі складної інформації, але слід бути обережним при інтерпретації вузлів, ґрунтуючись виключно на відображенні, так як структурні особливості, які кращим чином охоплює кількісний аналіз, можуть бути спотворені.

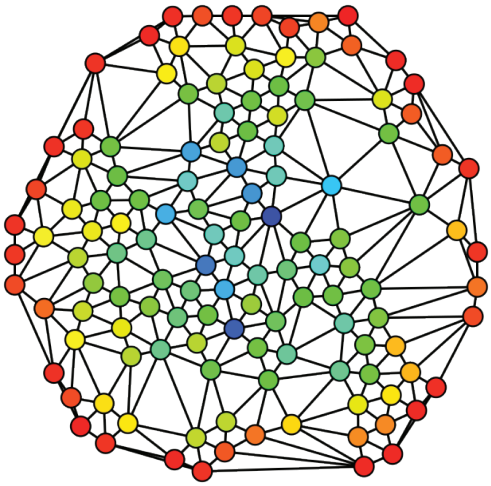


Рисунок 27.2. Класифікація зв'язків

У соціальних мережах існують поняття «збалансованих» та «незбалансованих» циклів. Під збалансованим циклом мають на увазі такий цикл, у якому результат усіх міток позитивний. Збалансовані цикли є групою людей, членам якої не хотілося б змінювати свою думку про інших членів групи. Незбалансовані цикли представляють групу людей, члени якої легко змінюють свою думку про інших членів групи.

> *Аналіз соціальних мереж активно використовується у розвідувальних, контррозвідувальних та правоохоронних заходах. Ця техніка дозволяє аналітикам відобразити на карті нелегальну чи приховану організацію, таку як шпигунське коло, організовану злочинну групу чи вуличну банду.*

Правоохоронні органи використовують програми масових систем електронного спостереження для генерації даних, необхідних для представлення цього аналізу в терористичних осередках та інших мережах, що мають відношення до національної безпеки.

У процесі мережного аналізу проводиться пошук у глибину на три вузли. Після того як завершилося початкове відображення соціальної мережі, виконується аналіз визначення структури мережі і, наприклад, лідера мережі. Це дозволяє військовим чи правоохоронним органам завдати нищівних ударів по захопленню чи знищенню найбільш значущих цілей, які займають лідерські позиції, що призводить до порушення функціонування мережі.

Можна досліджувати групові структури та потоки інформації на схемі мережі, фокусуючись на взаємозв'язках між об'єктами. Цей тип аналізу називається аналізом соціальних мереж. Організаційні теорії комбінуються з математичними моделями, що дає можливість зрозуміти динаміку цікавих для нас груп і організацій.

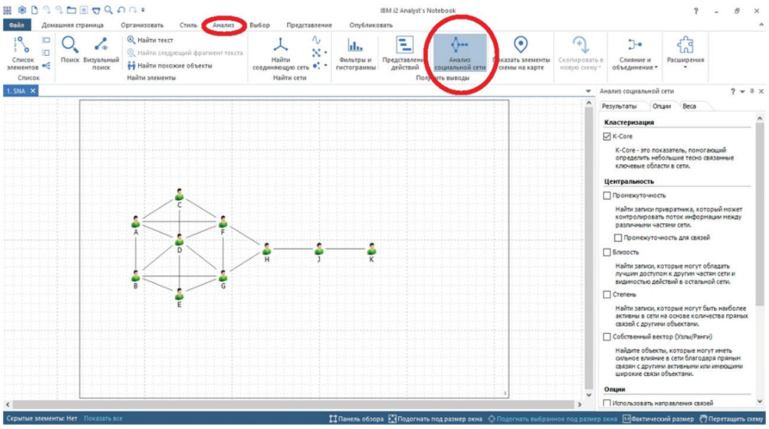
Використання «i2» в аналізі соціальних мереж

«i2» аналітика забезпечує потужний аналіз та надає допомогу можливості візуалізації, щоб допомогти підвищити продуктивність аналітики і скоротити час, необхідний для доставки високого значення інтелекту в межах швидко зростаючих наборів даних [5, с. 17]. У сфері кримінального аналізу i2, як правило, застосовується із програмними продуктами iBase, iBridge, iGlass, Analyst's Workstation. i2 Analyst's Workstation об'єднує можливості Analyst's Notebook, iBase, iGlass (компонента, що полегшує побудову графіків); дає змогу інтегруватися з GIS-технологіями (технологічна основа створення географічних інформаційних систем, що дозволяють реалізувати їхні функціональні можливості) та іншими технологіями аналітичної обробки даних, зокрема аналізу соціальних мереж. [6, с 10; 7, с. 60]

Структура мережі може визначати [8, с. 63]:

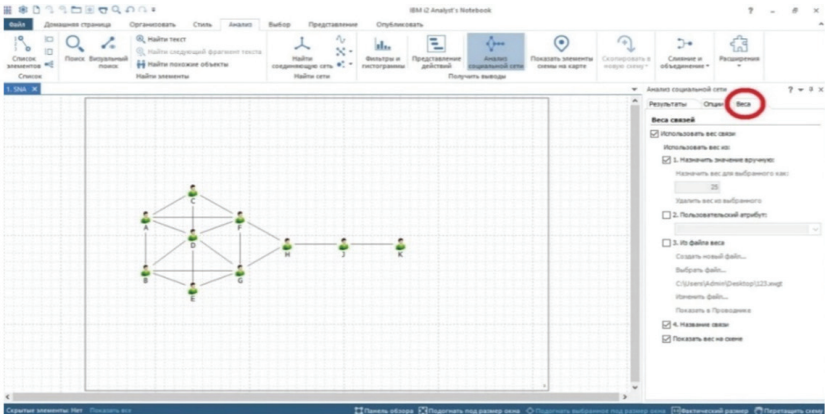
- *продуктивність мережі в цілому та її здатність досягти своїх ключових цілей;*
- *неочевидні характеристики мережі, наприклад існування меншої підмережі, що працює всередині мережі;*
- *взаємозв'язки між значущими людьми, що цікавлять нас, становище яких дозволяє найбільш сильно впливати на решту мережі;*
- *наскільки безпосередньо та швидко передається інформація між людьми у різних частинах мережі.*

У високоцентралізованій мережі є один об'єкт, який контролює усі інформаційні потоки. У менш централізованій мережі немає такої єдиної точки відмови. Люди можуть надсилати один одному інформацію, навіть якщо деякі канали зв'язку заблоковані. Зміна показника центральності, який використовується для аналізу схеми, дозволяє вивчити різну інформацію про елементи схеми.



Використовуючи i2 Analyst's Notebook, в опції «Аналіз соціальної мережі» можна вибирати показники центральності та задавати, виведення на екран результатів.

На сторінці «Вага» для зв'язків можна задати ваги, які мають силу з'єднань між реальними об'єктами. Ваги додаються як значення атрибута. Можливим є задати ваги вручну, отримати їх на основі існуючих атрибутів користувача і імпортувати їх з файлу «вага».



i2 Analyst's Notebook обчислює наступні показники центральності:

- *осередність,*
- *близькість,*
- *ступінь,*
- *власний вектор.*

Ці показники надають різну характеристику соціальних зв'язків у мережі. Також можна впливати на показники центральності, беручи до уваги напрям зв'язків та ваги, застосовані до них.

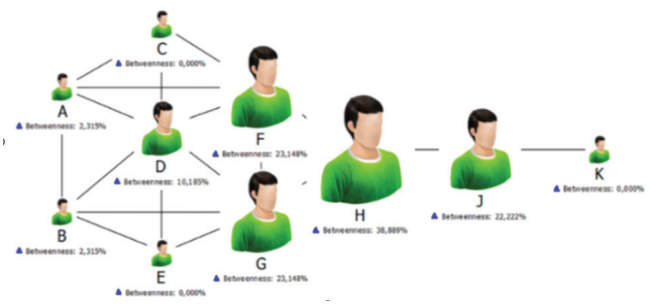
> ***Посередність:*** *«...чим більше людей залежать від мене для встановлення зв'язків з іншими людьми, тим більше влади я маю...».*

Центральність посередності вимірює кількість шляхів, що проходять через об'єкт. Цей показник може ідентифікувати об'єкти, які можуть контролювати потік інформації між різними частинами мережі. Такі об'єкти називають об'єктами-брамниками (воротар). Через об'єкт-брамник проходить багато шляхів, що дозволяє йому спрямовувати інформацію більшості інших об'єктів у мережі. В іншому варіанті шляхів, що проходять, може бути мало, але роль об'єкта може бути високою, якщо об'єкт знаходиться між різними мережевими кластерами.

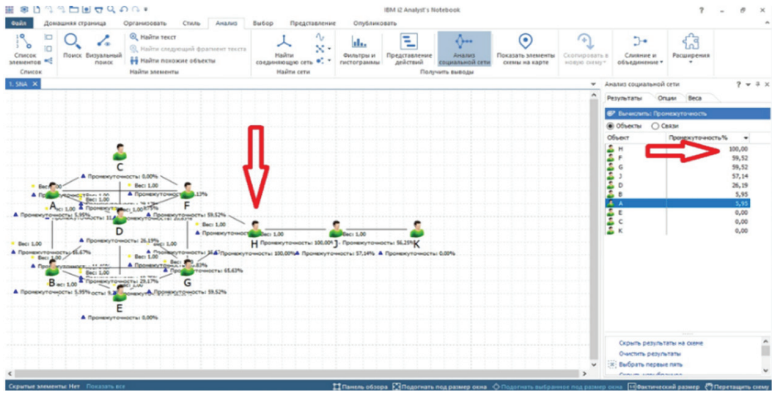
Центральність посередності вимірює як пряму, так і непряму близькість:

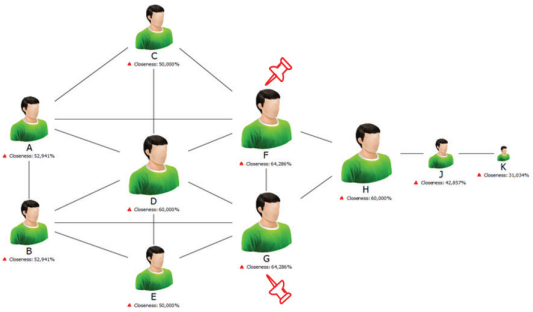
- *пряма близькість має місце, коли два об'єкти з'єднані зв'язком;*
- *непряма близькість має місце, коли інформація може передаватися від одного об'єкта до іншого тільки шляхом, що проходить через один або кілька проміжних об'єктів.*

Центральність посередності зв'язку вимірює кількість шляхів, що проходять через кожний зв'язок. Цей показник допоможе визначити ключові з'єднання впливу в мережі. Зв'язок, яким проходить багато шляхів, може бути маршрутом обміну інформацією між об'єктами.



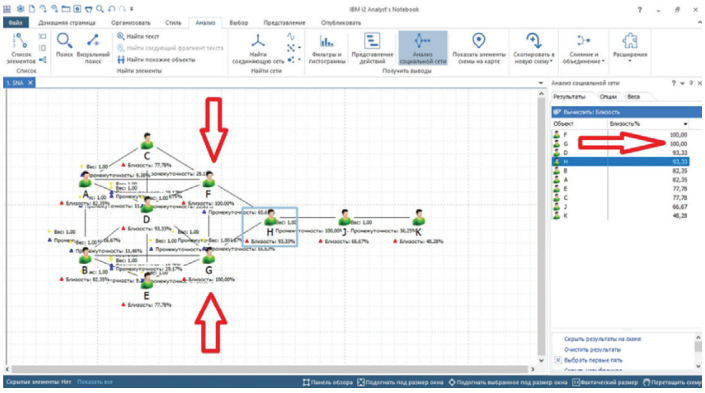
Функція посередність знаходить об’єкти, які можуть контролювати інформаційні потоки. У той час як об’єкт D має перелік прямих зв’язків, об’єкт H діє як «брокер». Не маючи його на тій позиції у мережі, об’єкти J та K були б відсторонені від інформації/





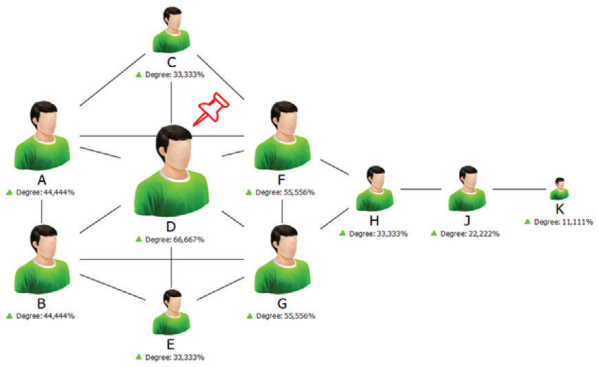
Близькість: *«…найкоротший шлях до всіх інших…».*

Центральність близькості вимірює близькість об’єкта до інших об’єктів у соціальній мережі. Об’єкт з високим ступенем центральності близькості шляху до інших об’єктів є найбільш коротким. Цей показник дозволяє їм передавати та отримувати повідомлення швидше за всі інші об’єкти в організації. Інформація проходить більшу відстань під час передачі до об’єкта на краю мережі, з’єднаного з невеликим числом інших об’єктів, або від нього. У таких об’єктів показник центральності близькості нижче.



Близькість знаходить об’єкти, які мають доступ до мережі. У той час як об’єкт D має багато зв’язків, реальна картина прямих та непрямих зв’язків що мають об’єкт F та G, надає їм мати доступ до всіх об’єктів в мережі, більш швидко, ніж любий інший об’єкт.

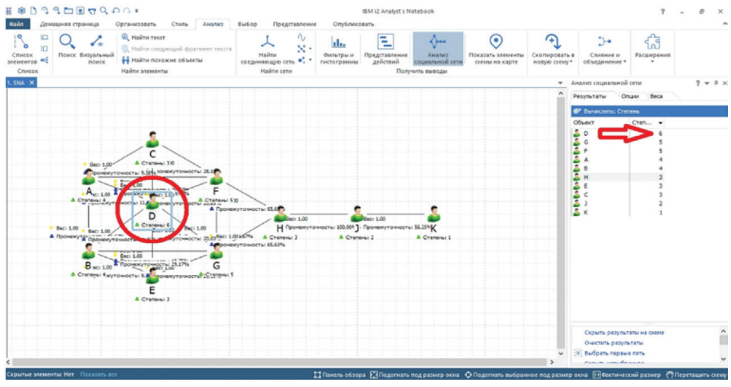
Ступінь: *«…найбільш прямі зв’язки, що має об’єкт…».*



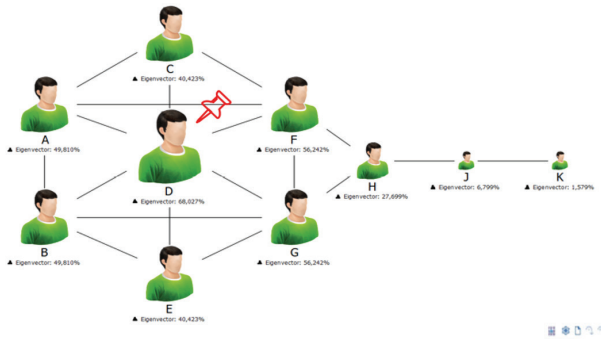
Ступінь центральності вимірює, наскільки об’єкти пов’язані з іншими об’єктами, підраховуючи кількість прямих зв’язків кожного об’єкта з іншими об’єктами у мережі. Вона може показати наскільки активний об’єкт та хто із учасників мережі активний з максимальним ступенем.

Ступінь знаходить об’єкти, що можуть бути найбільш активними в мережі, базуючись на кількості прямих зв’язків з іншими об’єктами. У цьому прикладі, об’єкт D має найбільшу кількість прямих зв’язків в мережі.

Власний вектор: *«…об’єкт є важливим якщо він є поєднаним з іншими важливими об’єктами…».*

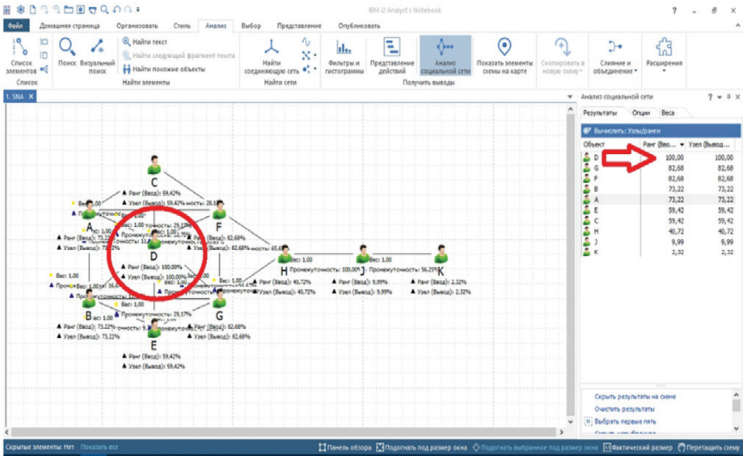


Власний вектор вимірює, наскільки об’єкт пов’язаний з іншими об’єктами і наскільки може безпосередньо вплинути на інші з’єднані об’єкти в мережі. Враховуються кількісні показники власного вектора об’єктів, з якими він пов’язаний. Наприклад, людина з високим показником власного вектора з великою ймовірністю знаходиться в центрі кластера ключових об’єктів, які самі мають високі показники власного вектора. Ця людина може безпосередньо зв’язуватися з цими ключовими об’єктами на відміну від людини з низьким показником власного вектора, що знаходиться на периферії мережі.



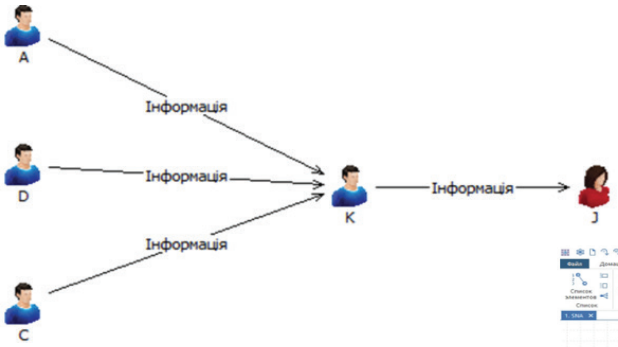
Власний вектор знаходить об'єкти, що можуть мати значний вплив в мережі на підставі наявності їх прямих зв'язків з іншими високо активними об'єктами. У цьому прикладі об'єкт D є в центрі кластеру ключових об'єктів A, B, F та G, що також мають високий рахунок власного вектору.

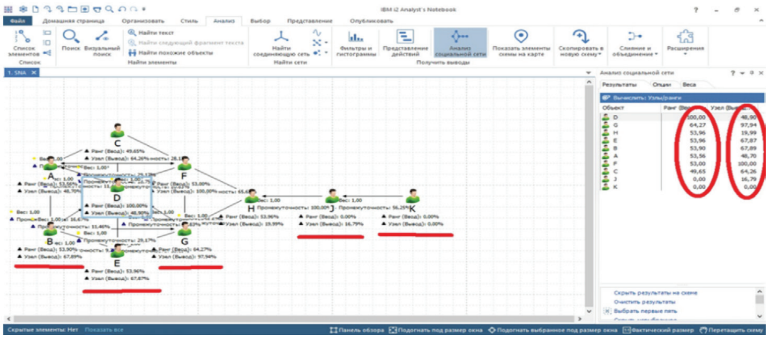
Концентратори та авторитети – терміни, що використовуються для опису двох показників власного вектора, що обчислюються в мережах із спрямованими зв'язками. Для визначення концентраторів враховують показники вихідних зв'язків, а визначення авторитетів – показники вхідних зв'язків. У концентратора з високим показником багато вихідних зв'язків до авторитетів з високим показником, а в авторитетів з високим показником – багато вхідних зв'язків від концентраторів з високим показником.



Напрям зв'язку

Спрямовані зв'язки можна враховувати під час розрахунку показників центральності. Зв'язок з визначеними стрілками напрямками представляє спрямований потік інформації між об'єктами або в одному напрямку або в обох напрямках. Цей показник може мати важливе відношення до того, як швидко передається інформація з однієї частини мережі до іншої. Наприклад, людина може отримувати інформацію від багатьох інших людей у мережі, але надсилати інформацію лише кільком обраним. Показник центральності для об'єкта, через який інформація передається в обох напрямках, вищий за цей показник для об'єкта, через який інформація передається в одному напрямку.

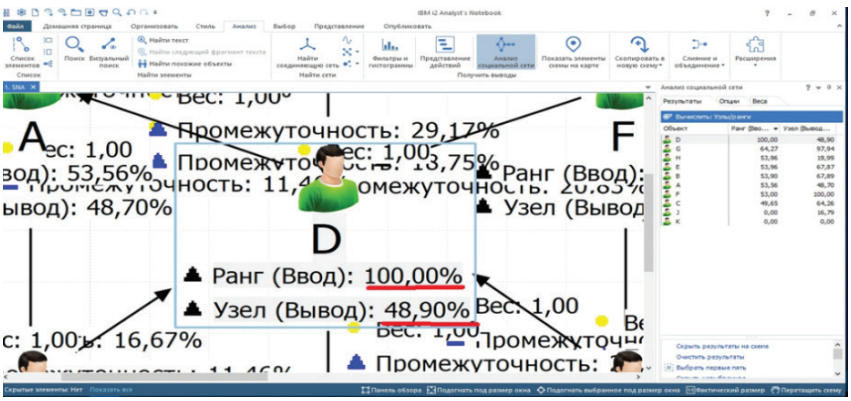




Ваги зв'язків

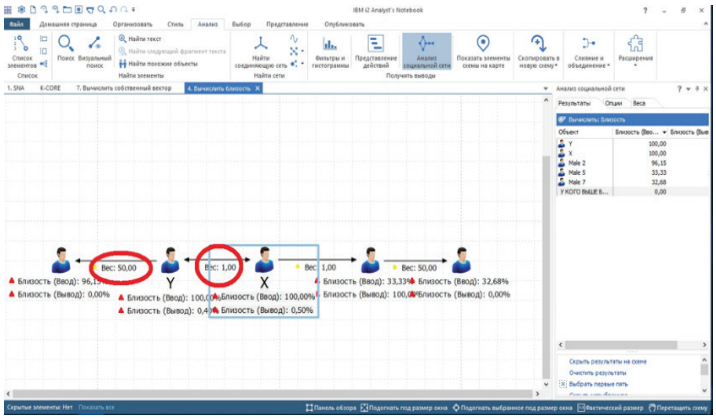
Не всі взаємозв'язки у мережі рівні. Наприклад, зв'язок між двома людьми, яких пов'язують родинні стосунки, може бути сильнішим, ніж зв'язок між двома діловими партнерами.

Для таких зв'язків можна ставити ваги, щоб під час аналізу соціальної мережі визначати силу зв'язків як і у реальному світі. Зважування ключових зв'язків у мережі може також означати, що об'єкти, які використовують ці зв'язки для передачі інформації, відіграють ключові ролі. Тому ваги зв'язків впливають на результати вимірювання центральності.



***K-Core** ядерність* – це показник, що допомагає визначити тісно пов'язані групи у мережі. К-ядро – це максимальна група об'єктів, всі з яких з'єднані щонайменше з іншими об'єктами в групі.

К-ядро – це показник, що допомагає визначити невеликі пов'язані ключові області мережі. Щоб бути включеним у К-ядро, об'єкт повинен бути пов'язаний щонайменше з іншими об'єктами в групі. Для визначення пов'язаних об'єктів не має значення, зі скількома іншими об'єктами вони з'єднані поза групою. «Максимальна» у визначенні означає, що нас цікавить найбільша кількість об'єктів, які мають необхідну мінімальну кількість сусідів у групі. Значення *k* іноді називають ядерністю групи.



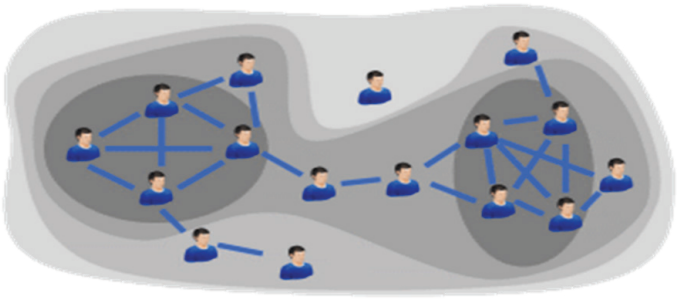
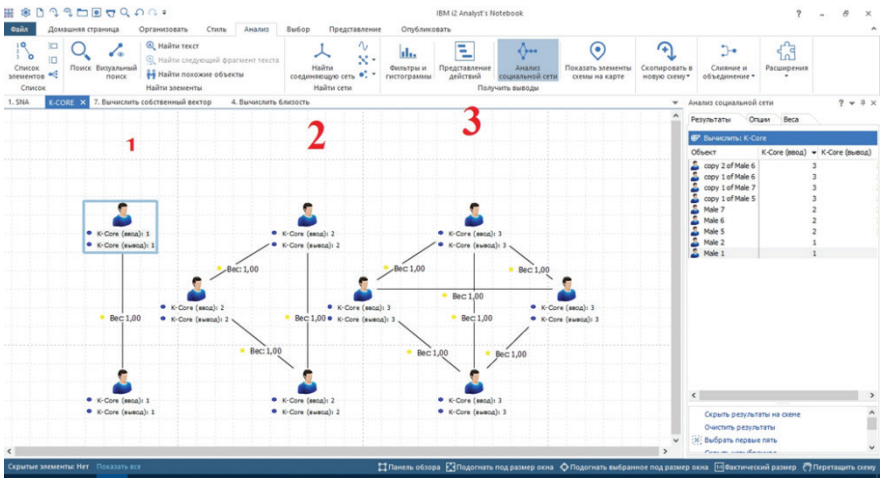


Рисунок 27.1. Розкладання простої мережі на К-ядра.

Наприклад, група є двоядром, якщо вона містить всі об'єкти, які з'єднані щонайменше з двома іншими об'єктами в групі. Аналогічно група є три-ядром, якщо вона містить усі об'єкти, пов'язані щонайменше з трьома іншими об'єктами в групі.

Будь-який об'єкт у три-ядрі повинен мати щонайменше три зв'язки з іншими членами три-ядра. Очевидно, що будь-який такий об'єкт має щонайменше два зв'язки з іншими членами три-ядра. Саме тому три-ядро є підмножиною (міститься всередині) дво-ядра. У загальному сенсі, К-ядро формує вкладену ієрархію групових об'єктів на схемі. Нуль-ядро (вся схема) містить одно-ядро, яке містить дво-ядро, яке містить три-ядро і так далі. Зі збільшенням *k* розміри ядра зменшуються, але зв'язність усередині ядра збільшується. К-ядра з найбільшими значеннями ядерності (*k-значення*) відображають найбільш зчеплені сегменти схеми.

Для обчислення результатів за великими схемами, i2 Analyst's Notebook потребує більше часу. Тривалість залежить від числа елементів на схемі та від числа показників центральності, які потрібно визначити. Якщо обчислення займає багато часу, можливим є працювати з іншими схемами, а обчислення продовжуватиметься у фоновому режимі. Щоб обчислення виконувалось у фоновому режимі, схема має залишатися відкритою; закриття схеми скасовує обчислення.



ВИКОРИСТАНІ ДЖЕРЕЛА

1. Pinheiro, Carlos A.R. (2011). Hoboke: *John Wiley & Sons*, 4.
2. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мережі: підручник [для вищих навчальних закладів]. Київ: CAMMIT-Книга, 2010. 708 с.
3. Снарский А.А., Ландэ Д.В. Моделирование сложных сетей: учебное пособие. Киев: Инжиниринг, 2015. 212 с. URL: http://dwl.kiev.ua/art/mss/mss-new.pdf
4. Albert-László, Barabási (2016). *Network Science*. Cambridge University Press.
5. Заєць О.М. Інститут аналітичного супроводження досудового розслідування кримінального провадження в Україні: сучасний стан і перспективи розвитку. *Вісник кримінального судочинства*. 2016. № 4. С. 17-25.
6. Основи кримінального аналізу: підручник / Бабенко А.М., Заєць О.М., Некрасов В.А., Ісмайлов К.Ю., Пефтієв Д.О. та ін.; за заг. ред. Користіна О.Є., 2020. 296 с.

7. Тактичний кримінальний аналіз: теорія та практика; навчальний посібник / О.Є. Користін, Н.П. Свиридюк, О.М. Цільмак, О.М. Заєць, К.Ю. Ісмайлов, В.А. Некрасов; МВС України, ДНДІ, ОДУВС. Одеса: РВВ ОДУВС, 2020. 216 с.
8. Мазуренко В.В., Штовба С.Д. Огляд моделей аналізу соціальних мереж. *Вісник Вінницького політехнічного інституту*. 2015. № 2. С. 62-74.
9. Ken, Cherven (2013). *Network Graph Analysis and Visualization with Gephi*. Packt Publishing.
10. Emden, R. Gansner, Eleftherios, Koutsoos & Stephen, North (January 5, 2015). *Drawing Graphs with dot*. Dot User's Manual. AT&T Bell Labs.
11. Ken, Cherven (2015). *Mastering Gephi Network Visualization*. Packt Publishing.
12. John W., Foreman (2013). *Data Smart*. Using Data Science to Transform Information into Insight. Wiley.

DOI: https://doi.org/10.36486/978-966-2310-66-5-28

Кожні кілька років з'являється новий програмний продукт, який має величезний вплив. Немає причин, щоб це зупинялося.

Даніель Бріклін

РОЗДІЛ 28
Операції з електронними таблицями і застосуванням Python

Анатолій Тімошин

Інформація, яка збирається аналітиком, відповідно до поставлених завдань, може бути різною за форматом, структурою та місцезнаходженням. Це можуть бути текстові, графічні, числові, звукові та відео дані. Наприклад, таблиці можуть поєднувати текст, числові значення, гіперпосилання, зображення і тощо. Отже, потрібно мати певний інструментарій (комп'ютерні програми або онлайн-сервіси в інтернеті), щоб ефективно опрацьовувати отриманий матеріал.

Найбільш потужним джерелом даних у роботі аналітика є інформаційні ресурси єдиної інформаційної системи МВС України та державні реєстри. Переважна більшість цих інформаційних ресурсів фактично є базами даних, тобто вони створені й зберігаються як набір таблиць, пов'язаних між собою. Технології роботи з базами даних передбачають пошук даних у таблицях за певними критеріями та інші операції з даними. Усе це нам підказує, що структурована інформація є найбільш ефективною для аналізу даних. Прикладами структурованих табличних даних є інформація від операторів зв'язку або працівників банку.

Зараз цінна інформація про певний об'єкт може бути отримана із соціальних мереж або шляхом пошуку на різних сайтах. Накопичену інформацію треба структурувати. Для цього, наприклад, можна побудувати асоціативну матрицю зв'язків (або потоків). Подальша візуалізація інформації відбувається в додатку i2 ANB. Щоб не будувати схеми вручну в i2 ANB, можна підготувати таблицю за такою структурою, коли можливий *імпорт* цієї таблиці в додаток (щось на зразок того, як виглядає таблиця банківських транзакцій).

Вважається, що найбільш сприятливим для аналізу й отримання певних гіпотез та висновків є зрозуміла та доречна *візуалізація* даних (наприклад, схема транзакцій або телефонних з'єднань в i2 ANB). Це безперечний факт. Але є багато питань, відповіді на які отримують шляхом аналізу даних у таблицях (обсяг даних, заголовки, типи даних, підрахунок записів за певними ознаками тощо). Таким чином, ми приходимо до того, що нам потрібні або табличній процесор – додаток, який оперує з рядками і стовпцями таблиць, або деяка програма, підготовлена, наприклад, у Python або R.

MS Excel

Прикладом одного з більш потужних і найпопулярніших інструментів для роботи з табличними даними є Excel. Можна згадати й такі табличні процесори, як: SuperCalc, LibreOffice Calc, GNumersc. Коли структуровані дані потрапляють в Excel, то кажуть про електронну таблицю. Частіше поняття «табличний процесор» та «електронна таблиця» ототожнюють, а конкретний набір даних в Excel можна називати діапазоном даних.

Робоча область (лист) будь-якого табличного процесора складається з комірок, які утворені за рахунок перетину рядків і стовпців. Рядки позначають цифрами (1, 2, 3, …), стовпці – буквами (A, B, C, …), і це дає змогу застосувати адресацію, коли кожна комірка листа має свій адрес (наприклад, A3, B1 тощо). Отже, для обробки й аналізу даних у комірках, можна звертатись за допомогою формул до вмісту комірок за їх адресою. До того ж адресація на листах електронної таблиці дозволяє звертатись до даних іншими інструментами, такими як мова Python (надалі це розглянемо більш детально).

Для розгляду базових інструментів Excel за перший приклад із табличних даних візьмемо звіт про кримінальні правопорушення із сайту Офісу Генерального прокурора, який розміщено відповідно до Положення про набори даних, що підлягають оприлюдненню у формі відкритих даних. Потрібну сторінку «Статистика» можна знайти за посиланням https://gp.gov.ua/ua/posts/statistika (рис. 28.1). Переходимо за вказаним (червоною стрілкою) посиланням на сторінку «Про зареєстровані кримі-

нальні правопорушення та результати їх досудового розслідування» і вибираємо один із файлів «Єдиний звіт про кримінальні правопорушення за …». Для кращого розуміння подальших дій рекомендується скачати один із файлів.

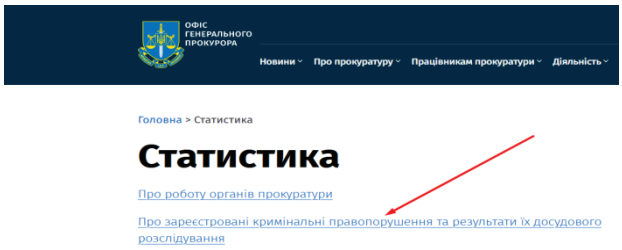


Рисунок 28.1. Сайт Офісу Генерального прокурора України

Вихідний формат файлу звіту на сайті є xlsx. Книга містить декілька листів, з яких виберемо лист 1. Цей лист містить загальні відомості про кількість зареєстрованих кримінальних правопорушень та результати їх досудового розслідування. Після скачування і відкриття файлу, краще перенести копію листа 1 в нову книгу.

Якщо ми наведемо курсор на будь-яку комірку таблиці з числовими значеннями, то побачимо, що там додано гіперпосилання. Для подальшої роботи з даними краще прибрати гіперпосилання. Зробити це можна так. Виділяємо всю область листа за допомогою кнопки «Виділити все» у верхньому лівому куті. На вкладці «Основне» знаходимо 7кнопку колекції «Очистити» й далі вибираємо «Очистити гіперпосилання» (рис. 28.2; указує синя стрілка).

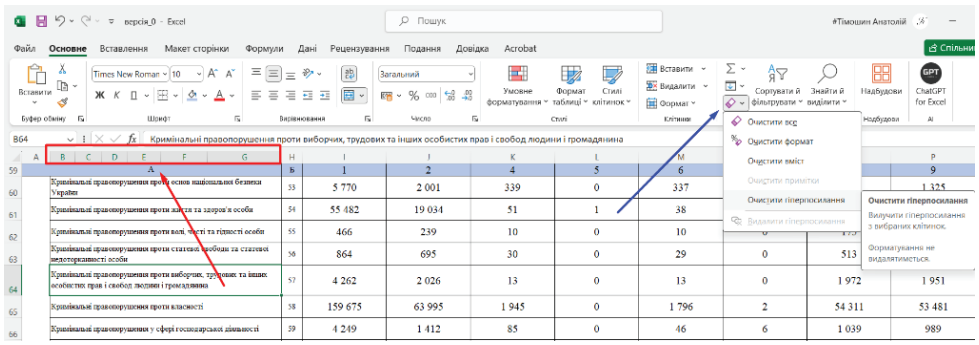


Рисунок 28.2. Очищення від гіперпосилань

Надалі будемо працювати лише з частиною даних на листі, а саме з таблицею 1.1, рядки таблиці «53»-«72», стовпці «1», «2», «3», «7», «20». Іншу інформацію видаляємо. Звертаємо вашу увагу на різницю щодо внутрішньої нумерації рядків і стовпців таблиці звіту та позначень рядків і стовпців у самому Excel.

Для подальших операцій фільтрації або сортування даних рекомендується спростити заголовок таблиці. Зауважимо, що стовпці таблиці мають внутрішню нумерацію: «А», «Б», «1», «2», …, «20» (рис. 28.2; рядок виділено сірим кольором). Дані стовпця «А» (рис. 28.2; указано червоною стрілкою) розташовано в об'єднаних стовпцях B – G. Скорегуємо стовпець «А» шляхом видалення стовпців А та С – G. На рис. 28.3 маємо остаточний вид таблиці. Заголовком стовпця «А» може слугувати таке: «Назва кримінальних правопорушень». У таблиці приведено 20 видів кримінальних правопорушень (внутрішня нумерація «53» – «72» у стовпці «Б»).

	A	B	C	D	E	F	G
1							
2							
3	Види кримінальних правопорушень	рядок	Обліковано кримінальних правопорушень у звітному періоді	Кримінальні правопорушення, у яких особам вручено повідомлення про підозру	Кримінальні правопорушення у провадженнях, досудове розслідування у яких зупинено відповідно до ст.ст. 280, 615 Кримінального процесуального кодексу України	Кримінальні правопорушення, за якими провадження направлені до суду (п.п. 2,3 ст. 283 Кримінального процесуального кодексу України)	Кримінальні правопорушення, у яких на кінець звітного періоду рішення не прийнято (про закінчення або зупинення)
4	А	Б	1	2	3	7	20
17	Кримінальні правопорушення у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інші кримінальні правопорушення проти здоров'я населення	65	36 382	26 992	137	24 251	11 963
18	Кримінальні правопорушення у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації	66	6 032	3 096	38	2 597	3 396

Рисунок 28.3. Скорегована таблиця

Аналіз таблиці почнемо із закріплення заголовку (рядки 1-4). Для цього поміщаємо курсор в комірку з адресом А5 і на вкладці «Подання» знаходимо кнопку колекції «Закріпити області» (рис. 28.4). Це дасть змогу завжди бачити заголовок при переміщенні по таблиці донизу.

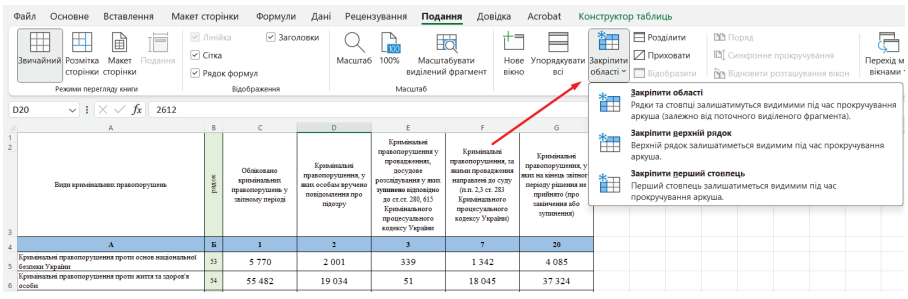
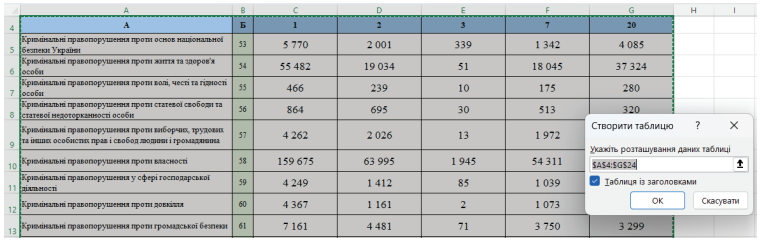


Рисунок 28.4. Закріплення заголовку

Перші кроки щодо аналізу даних краще розпочати з перетворення нашої таблиці на, так звану, «розумну» таблицю. Для цього виділяємо діапазон A4:M24, переходимо на вкладку «Вставлення» й обираємо кнопку «Таблиця» (рис. 28.5).



	Б	1	2	3	7	20
Кримінальні правопорушення проти основ національної безпеки України	53	5 770	2 001	339	1 342	4 085
Кримінальні правопорушення проти життя та здоров'я особи	54	55 482	19 034	51	18 045	37 324
Кримінальні правопорушення проти волі, честі та гідності особи	55	466	239	10	175	280
Кримінальні правопорушення проти статевої свободи та статевої недоторканності особи	56	864	695	30	513	320
Кримінальні правопорушення проти виборчих, трудових та інших особистих прав і свобод людини і громадянина	57	4 262	2 026	13	1 972	
Кримінальні правопорушення проти власності	58	159 675	63 995	1 945	54 311	
Кримінальні правопорушення у сфері господарської діяльності	59	4 249	1 412	85	1 039	
Кримінальні правопорушення проти довкілля	60	4 367	1 161	2	1 073	
Кримінальні правопорушення проти громадської безпеки	61	7 161	4 481	71	3 750	3 299

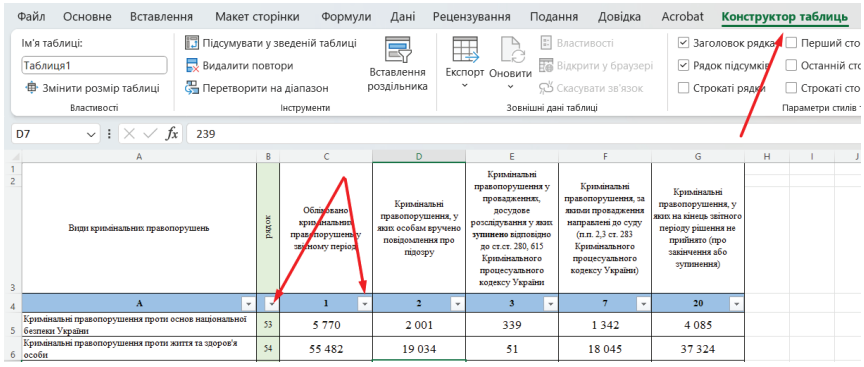
Рисунок 28.5. Створення «розумної» таблиці

У результаті цієї операції в рядку 4 (рядок із внутрішніми номерами стовпців таблиці) отримаємо позначки фільтру (рис. 28.6; указують червоні стрілки) і в Excel з'явиться нова вкладка «Конструктор таблиць» (рис. 28.6; синя стрілка).

На вкладці «Конструктор таблиць» увімкнемо «Рядок підсумків». Під останнім рядком таблиці з'явиться рядок підсумків (рис. 28.7).

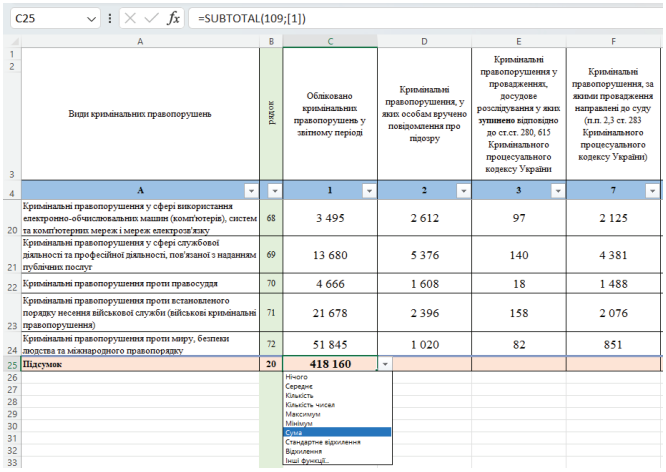
Поставимо курсор у комірку рядка підсумків стовпця з номером «1» (Обліковано кримінальних правопорушень у звітному періоді). Це комірка з адресою C25. З правого боку комірки побачимо значок колекції (до речі, цей значок схожий на значок фільтру).

У відкритій колекції можна бачити назви тих проміжних підсумків, які можна отримати: середнє, кількість, кількість чисел, максимум, мінімум, сума тощо. Обираємо «сума» й отримуємо кількість кримінальних правопорушень за звітний період.



Види кримінальних правопорушень	рядок	Обліковано кримінальних правопорушень у звітному періоді	Кримінальні правопорушення, у яких особам вручено повідомлення про підозру	Кримінальні правопорушення у провадженнях, досудове розслідування у яких зупинено відповідно до ст.ст. 280, 615 Кримінального процесуального кодексу України	Кримінальні правопорушення, за якими провадження направлені до суду (п.п. 2,3 ст. 283 Кримінального процесуального кодексу України)	Кримінальні правопорушення, у яких на кінець звітного періоду рішення не прийнято (про закінчення або зупинення)
A		1	2	3	7	20
Кримінальні правопорушення проти основ національної безпеки України	53	5 770	2 001	339	1 342	4 085
Кримінальні правопорушення проти життя та здоров'я особи	54	55 482	19 034	51	18 045	37 324

Рисунок 28.6. Конструктор таблиць



	рядок	1	2	3	7
Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку	68	3 495	2 612	97	2 125
Кримінальні правопорушення у сфері службової діяльності та професійної діяльності, пов'язної з наданням публічних послуг	69	13 680	5 376	140	4 381
Кримінальні правопорушення проти правосуддя	70	4 666	1 608	18	1 488
Кримінальні правопорушення проти встановленого порядку несення військової служби (військові кримінальні правопорушення)	71	21 678	2 396	158	2 076
Кримінальні правопорушення проти миру, безпеки людства та міжнародного правопорядку	72	51 845	1 020	82	851
Підсумок	20	418 160			

Рисунок 28.7. Створення рядка підсумків

Усі ці значення обчислюються за допомогою однієї функції SUBTOTAL. Синтаксис функції наступний: SUBTOTAL(номер функції; діапазон). Номер функції (обов'язковий аргумент) – число від 1 до 11 або від 101 до 111, що вказує, яку функцію використовувати для проміжних підсумків. Аргументи від 1 до 11 працюють із прихованими вручну рядками, а аргументи від 101 до 111 при підрахунку ігнорують приховані рядки. Зв'язок між номером обов'язкового аргументу функції SUBTOTAL та функцією в Excel наступний:

1 (101) – AVERAGE (середнє)
2 (102) – COUNT (кількість)
3 (103) – COUNTA (кількість чисел)
4 (104) – MAX
5 (105) – MIN
9 (109) – SUM (сума)

Для підрахунку кількості записів таблиці вибирають «кількість». У нашому прикладі для цього можна використати комірку B25 у рядку підсумків.

Рядок підсумків працює, коли робимо фільтрацію записів. Для прикладу, серед указаних видів кримінальних правопорушень залишимо лише правопорушення щодо особи (це можуть бути рядки «54», «55», «56», «57», «58» за внутрішньою нумерацією). Клацаємо на позначку фільтру в комірці B4 і вибираємо необхідне (рис. 28.8). Залишаються тільки 4 рядка, і в рядку підсумків сума правопорушень буде відповідати вибраним рядкам (рис. 28.9). При тому позначка фільтру в комірці B4 змінить зображення.

Нескладно повернути всі рядки знову. Клацаємо значок того ж фільтру й обираємо «Виділити все».

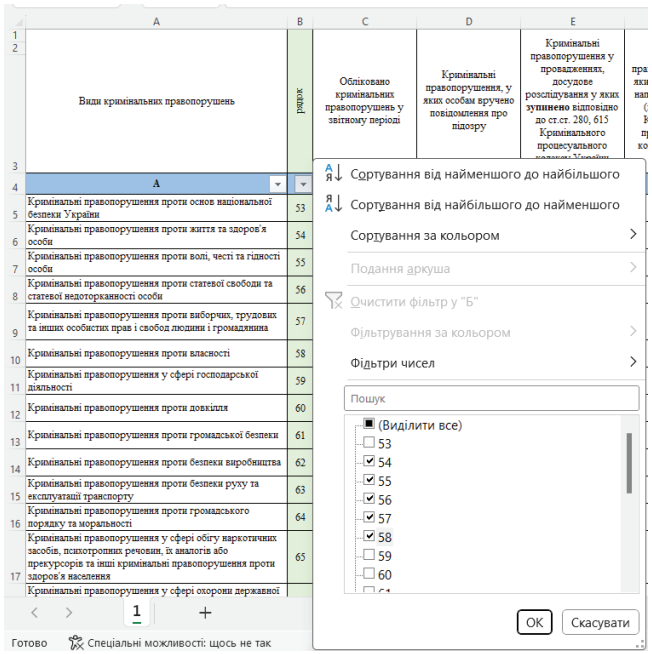


Рисунок 28.8. Використання фільтрів

Щоб порівняти кількість облікованих правопорушень за їх типом, можна скористатися сортуванням (наприклад, від найменшого до найбільшого). Відповідний фільтр – у комірці С4. У результаті сортування знаходимо, що найменша кількість облікованих кримінальних правопорушень проти волі, честі та гідності особи, найбільша – проти власності.

Якщо ми знову хочемо повернути таблицю до початкового стану, то на цей випадок якраз потрібен стовпець «Б». Достатньо відсортувати цей стовпець за зростанням номерів.

Види кримінальних правопорушень	рядок	Обліковано кримінальних правопорушень у звітному періоді	Кримінальні правопорушення, у яких особам вручено повідомлення про підозру	Кримінальні правопорушення у провадженнях, досудове розслідування у яких зупинено відповідно до ст.ст. 280, 615 Кримінального процесуального кодексу України	Кримінальні правопорушення, за якими провадження направлені до суду (п.п. 2,3 ст. 283 Кримінального процесуального кодексу України)	Кримінальні правопорушення, у яких на кінець звітного періоду рішення не прийнято (про закінчення або зупинення)
A	B	1	2	3	7	20
Кримінальні правопорушення проти життя та здоров'я особи	54	55 482	19 034	51	18 045	37 324
Кримінальні правопорушення проти волі, честі та гідності особи	55	466	239	10	175	280
Кримінальні правопорушення проти статевої свободи та статевої недоторканності особи	56	864	695	30	513	320
Кримінальні правопорушення проти виборчих, трудових та інших особистих прав і свобод людини і громадянина	57	4 262	2 026	13	1 972	2 277
Кримінальні правопорушення проти власності	58	159 675	63 995	1 945	54 311	103 270
Підсумок	5	44 150	85 989	2 049	75 016	143 471

Рисунок 28.9. Вибрані рядки після застосування фільтру

Розглянемо на прикладі нашої таблиці поняття *умовного форматування*. Нехай у стовпці облікованих кримінальних правопорушень (стовпець «1») потрібно виділити іншим кольором ті комірки, значення в яких більше за їх середнє. Середнє значення кількості правопорушень по видах правопорушень знайдемо в рядку підсумків (рис. 28.10).

	A		1	2
17	Кримінальні правопорушення у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інші кримінальні правопорушення проти здоров'я населення	65	36 382	26 992
18	Кримінальні правопорушення у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації	66	6 032	3 096
19	Кримінальні правопорушення проти авторитету органів державної влади, органів місцевого самоврядування, об'єднань громадян та кримінальні правопорушення проти журналістів	67	23 079	14 895
20	Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку	68	3 495	2 612
21	Кримінальні правопорушення у сфері службової діяльності та професійної діяльності, пов'язаної з наданням публічних послуг	69	13 680	5 376
22	Кримінальні правопорушення проти правосуддя	70		1 608
23	Кримінальні правопорушення проти встановленого порядку несення військової служби (військові кримінальні правопорушення)	71		2 396
24	Кримінальні правопорушення проти миру, безпеки людства та міжнародного правопорядку	72		1 020
25	Підсумок	20	20 908	

Нічого
Середнє
Кількість
Кількість чисел
Максимум
Мінімум
Сума
Стандартне відхилення
Відхилення
Інші функції...

Рисунок 28.10. Визначення середнього значення

Далі, виділяємо діапазон комірок С4:С24 і на панелі інструментів (вкладка «Основне») тиснемо кнопку «Умовне форматування» (рис. 28.11). Обираємо «Правила виділення клітинок» і далі беремо «Більше». З'явиться додаткове вікно (рис. 28.12), у якому треба вказати значення або адрес комірки з цим значенням. Відповідні комірки діапазону С4:С24 поміняють колір на блідо-червоний (колір можна змінити). Порівняння буде з середнім значенням, яке знаходиться в комірці С25, що і вказується в діалоговому вікні.

Завдяки умовному форматуванню ми можемо сконцентрувати увагу на тих комірках, які підпадають під певне правило і змінюють колір. У нашому прикладі ми можемо проглянути ті види правопорушень, кількість яких вище за середнє.

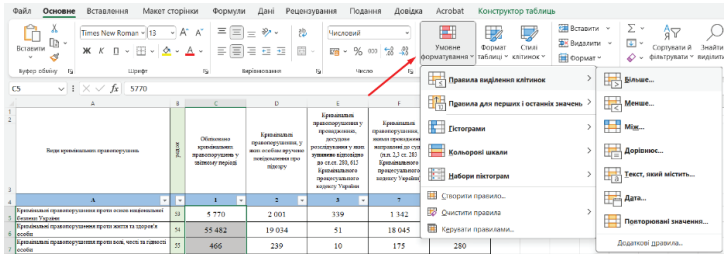


Рисунок 28.11. Умовне форматування

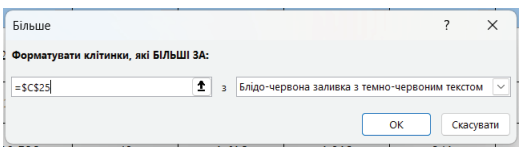


Рисунок 28.12. Зміна кольору

Щоб прибрати умовне форматування з певних комірок, достатньо виділити їх і вибрати «Очистити правила» (рис. 28.11).

Іноді потрібно швидко оцінити числові дані в порівнянні один з одним. Знову можна скористатися умовним форматуванням і вибрати «Гістограми», «Градієнтна заливка» (або «Суцільна заливка»). Відбудеться відносне зафарбовування комірок залежно від значень (рис. 28.13).

Статистичні дані краще представляти в більш наочній і зручній для сприйняття формі – у вигляді діаграм. Це спрощує розуміння відносин між рядами даних великого обсягу. Excel підтримує різні типи діаграм – звичайні стовпчасті, лінійчаті, секторні, гістограми, пелюсткові і т. ін. Вибір типу діаграми в кожному випадку залежить від характеру даних та їх аналізу, задач, які ми хочемо вирішити.

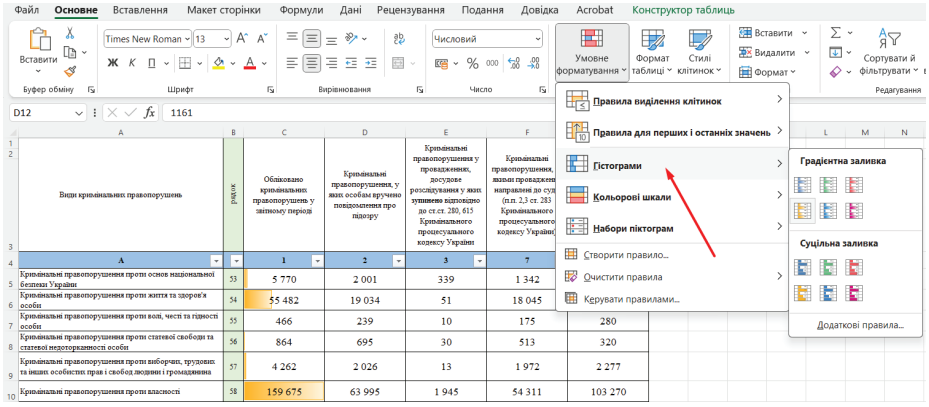


Рисунок 28.13. Порівняння числових даних

Пропонують 3 базові види аналізу. Для візуалізації кожного з них можна використовувати лише певні види діаграм: інші спотворять сприйняття даних і просто не допоможуть побачити потрібне.

Рейтинг – цей вид аналізу ми використовуємо, коли потрібно порівняти між собою кілька показників. Тобто, це будь-яке кількісне порівняння за шкалою, градація від більшого до меншого. Використовують стовпчасті, лінійчаті діаграми, гістограми. На вибір впливає об'єм даних: якщо менше 10 точок, то обирають звичайну стовпчасту. Якщо підписи даних завеликі, то використовують горизонтальну гістограму.

Динаміка – такий вид аналізу ми вибираємо, коли потрібно простежити зміну одного показника. Використовують діаграму лінійчату або гістограму залежно від кількості даних(точок): якщо їх більше 10, то краще брати лінійчату.

Структура – використовується у випадках, коли важливо розділити щось ціле на частки й показати обсяг кожної. Для цього виду аналізу обирають секторну діаграму.

Побудуємо звичайну стовпчасту діаграму за результатами досудового розслідування для усієї сукупності кримінальних правопорушень. Підготуємо діапазон даних діаграми – у рядку підсумків для кожного стовпця таблиці візьмемо Суму (рис. 28.14). Виділяємо комірки C25:G25, заходимо на вкладку «Вставлення» і вибираємо значок колекції.

В отриманій діаграмі змінюємо назву й легенду (рис. 28.15). На рис. 28.16 можна побачити, яким чином можна редагувати назву рядів даних.



	Види кримінальних правопорушень	рядок	Обліковано кримінальних правопорушень у звітному періоді	Кримінальні правопорушення, у яких особам вручено повідомлення про підозру	Кримінальні правопорушення у провадженнях, досудове розслідування у яких зупинено відповідно до ст.ст. 280, 615 Кримінального процесуального кодексу України	Кримінальні правопорушення, за якими провадження направлені до суду (п.п. 2,3 ст. 283 Кримінального процесуального кодексу України)	Кримінальні правопорушення, у яких на кінець звітного періоду рішення не прийнято (про закінчення або зупинення)
	A	B	C	D	E	F	G
			1	2	3	7	20
23	Кримінальні правопорушення проти встановленого порядку несення військової служби (військові кримінальні правопорушення)	71	21 678	2 396	158	2 076	19 436
24	Кримінальні правопорушення проти миру, безпеки людства та міжнародного правопорядку	72	51 845	1 020	82	851	50 911
25	Підсумок	20	418 160	160 954	3 776	140 700	273 137

Рисунок 28.14.Виділення діапазону даних

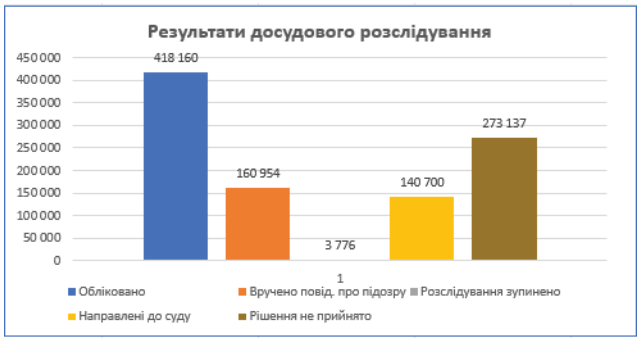


Рисунок 28.15. Зміна назви і легенди діаграми

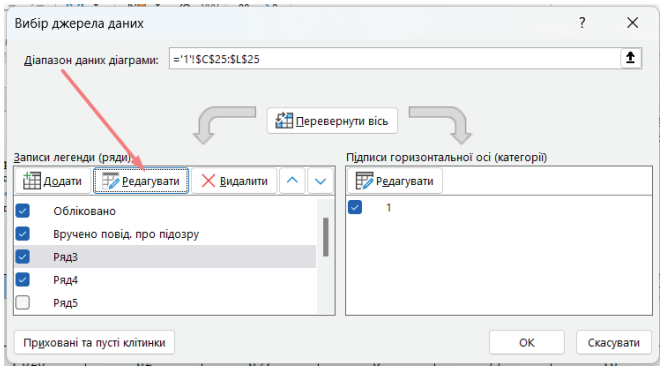


Рисунок 28.16. Редагування назви рядів даних

У наступному прикладі діаграми за показник візьмемо кількість облікованих кримінальних правопорушень по кожному виду правопорушень. Кількість точок даних перевищує 10, тому виберемо лінійчату діаграму (рис. 28.17).

Серед наступних можливостей Excel при аналізі структурованих даних потрібно розглянути ***зведені таблиці***.

За наступний приклад візьмемо таблицю банківських транзакцій (рис. 28.18). Таблиця має 4 поля: *Джерело, Призначення, Дата час, Сума коштів*. Поля Джерело і Призначення містять номера рахунків, але формат цих полів встановимо як текстовий – це дасть змогу залишити нуль на початку рахунків (інакше Excel буде розуміти це як число і нуль відкине).



Рисунок 28.17. Побудова лінійчатої діаграми

Узагалі, на початку аналізу даних завжди треба визначитися з форматом полів.

Таблиця має більше тисячі записів, і щоб здійснити початковий аналіз по рахунках, діапазон даних таблиці відразу перетворимо в «розумну таблицю». Нагадаємо, що це робиться через вкладку «Вставлення», «Таблиця», після чого з'явиться додаткова вкладка «Конструктор таблиць». До речі, якщо курсор помістити за межі таблиці, ця вкладка зникає.

	A	B	C	D
1	Джерело	Призначення	Дата час	Сума коштів
2	01223854840	01429256054	01 01 2020 9:43	2345,00
3	01223854840	01364558175	01 01 2020 19:54	1365,00
4	01223854840	01914715106	01 01 2020 22:42	19785,00
5	01223854840	01914715106	02 01 2020 9:38	24362,00
6	07989967213	07497762938	02 01 2020 11:02	10653,00
7	01223854840	07989967213	02 01 2020 12:20	2463,00
8	01223854840	01699944965	02 01 2020 15:13	34671,00
9	01223854840	07497762938	02 01 2020 16:38	24531,00
10	01223854840	01347578654	02 01 2020 19:58	1362,00

Рисунок 28.18. Таблиця банківських транзакцій

Увімкнемо рядок підсумків й оцінимо кількість записів у таблиці (комірка B1596) та загальну суму транзакцій (комірка D1596) (рис. 28.19).

	A	B	C	D
1	Джерело	Призначення	Дата час	Сума коштів
1574	01223859234	07497762938	30 03 2020 12:33	42617,00
1575	01638782715	01349247866	30 03 2020 13:37	35261,00
1576	07497762938	01973105544	30 03 2020 13:44	84938,00
1577	01638782715	01438164750	30 03 2020 13:57	2738,00
1578	01638782715	01854883676	30 03 2020 14:24	35627,00
1579	01223859234	07989967213	30 03 2020 14:59	9684,00
1580	01223859234	01223854840	30 03 2020 16:01	2781,00
1581	01638782715	01854883676	30 03 2020 17:15	62938,00
1582	07497762938	01434069006	30 03 2020 18:23	2345,00
1583	01223854840	01699944965	30 03 2020 18:45	1365,00
1584	01638782715	01438164750	30 03 2020 19:08	19785,00
1585	01223854840	07497762938	30 03 2020 19:15	24362,00
1586	07497762938	01223573298	30 03 2020 19:17	10653,00
1587	01223854840	01309657924	30 03 2020 20:00	2463,00
1588	01223854840	01699944965	30 03 2020 21:46	34671,00
1589	01223854840	01223859234	30 03 2020 21:48	24531,00
1590	01223854840	07497762938	30 03 2020 22:20	1362,00
1591	01223854840	07989967213	31 03 2020 8:07	2463,00
1592	01638782715	01948474016	31 03 2020 9:23	1231,00
1593	01638782715	01463160895	31 03 2020 14:43	34928,00
1594	07497762938	01830520901	31 03 2020 14:44	5732,00
1595	01223854840	01885779839	31 03 2020 18:36	82413,00
1596	Підсумок	1594		42578584,00

Рисунок 28.19. Оцінка таблиці банківських транзакцій

Щоб проглянути підсумкові дані щодо конкретного рахунку (наприклад, 01223854840), з якого перераховувалися кошти, скористаємося фільтром стовпця «Джерело». Значення в комірках B1596 (кількість транзакцій) і D1596 (сума коштів) змінилися (рис. 28.20).

	A	B	C	D
1	Джерело	Призначення	Дата час	Сума коштів
1587	01223854840	01309657924	30 03 2020 20:00	2463,00
1588	01223854840	01699944965	30 03 2020 21:46	34671,00
1589	01223854840	01223859234	30 03 2020 21:48	24531,00
1590	01223854840	07497762938	30 03 2020 22:20	1362,00
1591	01223854840	07989967213	31 03 2020 8:07	2463,00
1595	01223854840	01885779839	31 03 2020 18:36	82413,00
1596	Підсумок	533		13664524,00

Рисунок 28.20. Використання фільтру

Але якщо ми хочемо порівняти кількість транзакцій і суму перерахованих коштів щодо різних рахунків, то краще створити зведену таблицю. Для цього на вкладці «Конструктор таблиць» в розділі «Інструменти» тиснемо кнопку «Підсумувати у зведеній таблиці» (рис. 28.21). Excel запропонує розташувати зведену таблицю в новому аркуші або в наявному. За замовчуванням це новий аркуш (краще вибрати цей варіант).

Наступним кроком, у новому аркуші, з'явиться макет зведеної таблиці (рис. .22, ліворуч) – це *область звіту* (початок звіту – комірка A3) та *панель налаштування* зведеної таблиці (рис. 28.22, праворуч). Панель налаштування складається з області з полями таблиці (зверху) та чотирма областями: *Фільтри, Рядки, Стовпці, Значення*.

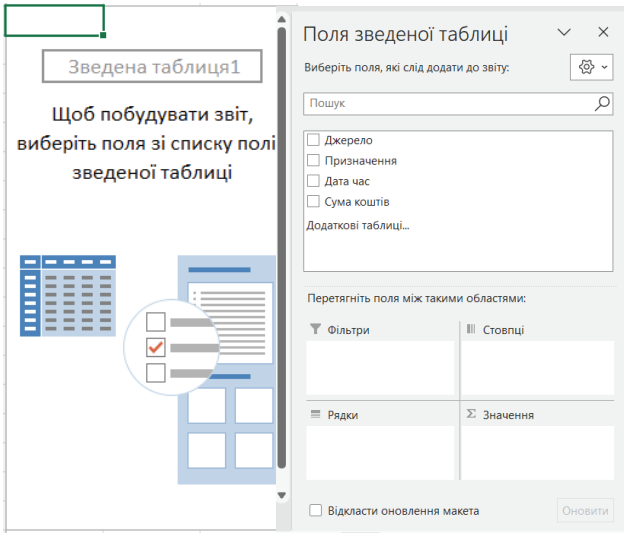


Рисунок 28.22. Макет зведеної таблиці

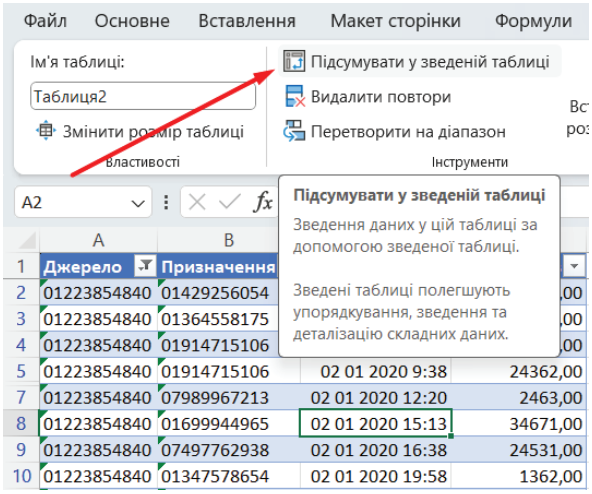


Рисунок 28.21. Визначення підсумку у зведеній таблиці

Як тільки в панелі налаштування ми поставимо прапорець на полі «Джерело», то в області «Рядки» панелі з'явиться рядок «Джерело» і в області звіту з'являться рядки з номерами унікальних рахунків. Поставимо прапорець на полі «Сума коштів». В області «Значення» з'явиться рядок «Сума з Сума коштів» (рис. 28.23).

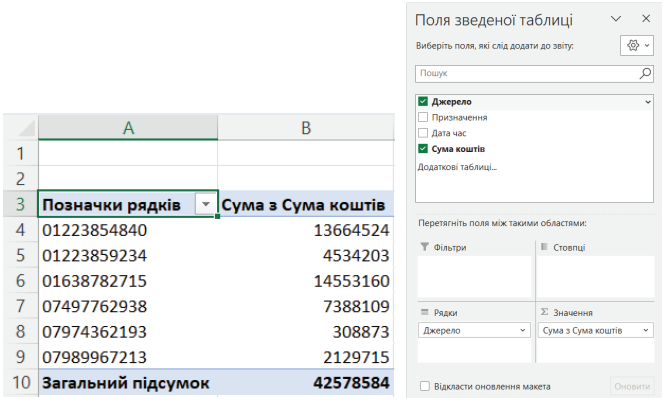


Рисунок 28.23. Додаткове налаштування зведеної таблиці

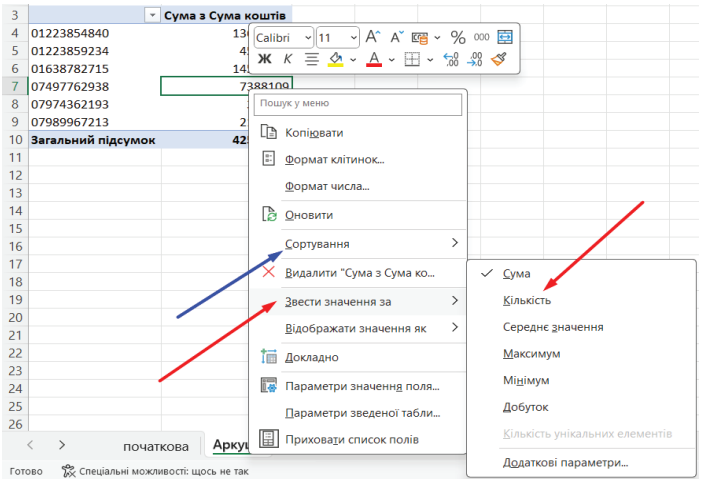


Рисунок 28.24. Сортування даних у зведеній таблиці

В області звіту з'явиться стовпчик зі зведеними сумами перерахованих коштів для кожного рахунку. За умови значної кількості рядків у зведеній таблиці, їх можна відсортувати. Для цього потрібно поставити курсор на будь-яку комірку другого стовпця, натиснути праву клавішу миші і вибрати «Сортування» (рис. 28.24). Суми коштів можна змінити на кількість транзакцій (рис. 28.24).

Зведені таблиці (для цього прикладу) допоможуть швидко визначити рахунок, з якого (на який) надійшла найбільша (найменша) сума коштів або отримати подібну інформацію щодо кількості транзакцій.

Зведену таблицю перерахованих коштів по датах краще зробити, коли дата і час розділені на окремі стовпці. Для цього на вкладці «Дані» є кнопка «Текст за стовпцями», але спочатку треба додати порожній стовпець праворуч (для значень часу) та виділити стовпець «Дата час» (рис. 28.25).

Якщо потрібно швидко знайти комірку (або комірки) з конкретним текстом чи значенням, причому, може бути відома частина

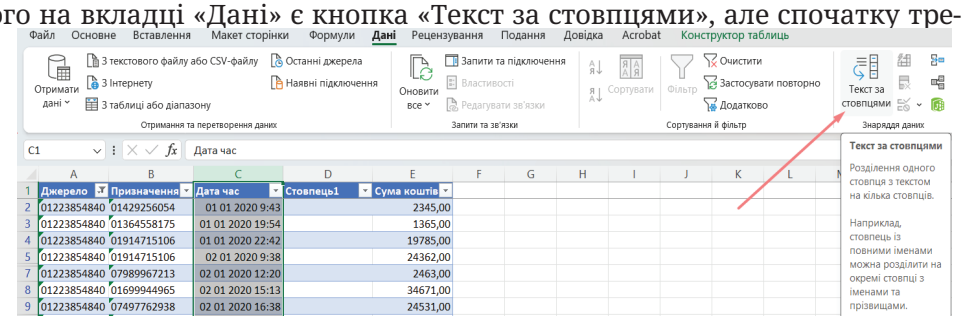
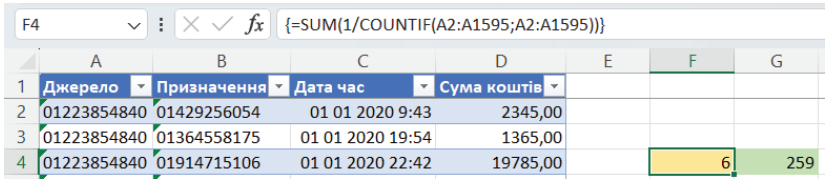


Рисунок 28.25. Створення додаткового стовпця

тексту, то знову використаємо умовне форматування. Спочатку виділяємо потрібний діапазон із даними, тиснемо кнопку «Умовне форматування», обираємо «Правила виділення клітинок» і беремо «Текст, який містить …». З'явиться додаткове вікно, у якому треба вказати бажаний текст (або його частину). Відповідні комірки автоматично змінять колір, вказуючи на шукані дані. Щоб зібрати комірки з іншим кольором в одну групу, можна виконати сортування за кольором комірки (через кнопку фільтра).

> *За умови, коли таблиця містить велику кількість записів (рядків), аналіз даних потребує використання формул.*

На прикладі таблиці банківських транзакцій спочатку поставимо питання визначити кількість унікальних рахунків стовпця «Джерело» та кількість унікальних рахунків стовпця «Призначення». Для підрахунку числа унікальних значень у діапазоні використовують формулу масиву: =SUM(1/COUNTIF (масив; масив)). Отже, в окремій від таблиці комірці (наприклад, F4) вводимо формулу =SUM(1/COUNTIF (A2:A1595; A2:A1595)) і тиснемо комбінацію клавіш <Ctrl+Shift+Enter>. Отримаємо число 6 (рис. 28.26). Це кількість унікальних рахунків стовпця «Джерело» (їх було видно раніше, у зведеній таблиці). Аналогічно знаходимо кількість унікальних рахунків стовпця «Призначення» (у нашій таблиці їх 259), замінивши у формулі діапазон (масив) на B2:B1595.



	A	B	C	D	E	F	G
1	Джерело	Призначення	Дата час	Сума коштів			
2	01223854840	01429256054	01 01 2020 9:43	2345,00			
3	01223854840	01364558175	01 01 2020 19:54	1365,00			
4	01223854840	01914715106	01 01 2020 22:42	19785,00		6	259

Рисунок 28.26. Використання формули суми масиву

Як бачимо, кількість унікальних рахунків у стовпці B велика і визначити кількість повторювання певного рахунку в стовпці можна через формулу. Наприклад, для підрахунку кількості повторювання рахунку 01699944965 візьмемо формулу =COUNTIF(B2:B1595;"*4965"). Знак зірочки (*) у формулі означає будь-які символи. Його використовують, коли частину рядка невідомо.

До прикладу, нам потрібно оцінити суму переказів, які перевищують певне значення. Це можна зробити за допомогою умовного форматування – виділити такі комірки в стовпці D, відфільтрувати за кольором комірок, потім у рядку підсумків побачимо необхідне значення. А можна використати формулу: =SUMIF(E2:E1595;">30000").

Розв'яжемо ще таку задачу. Потрібно порахувати суму коштів, які залишились на певному рахунку (за умови, що з цього рахунку перераховувалися кошти та надходили кошти на цей рахунок). Шляхом фільтрації по стовпцю A можна знайти суму коштів, що були перераховані, а фільтрація по стовпцю B дасть кошти, які надійшли на рахунок. Різниця отриманих значень дасть шукану суму. Цю задачу краще вирішити за допомогою формули:

=SUMIF(A2:A1595;"*2938";D2:D1595) – SUMIF(B2:B1595;"*2938";D2:D1595).

Досить часто при аналізі таблиць використовують такі функції пошуку та підрахунку необхідних значень, як VLOOKUP, MATCH, INDEX, COUNT, COUNTA. Приведемо стислу довідку про ці функції.

VLOOKUP (ВПР) – функція пошуку та вилучення значення зі стовпця. Підтримує підстановочні знаки «*» та «?». Нагадаємо, що знак «*» означає довільну кількість символів, а знак «?» – один довільний символ. Наприклад, фраза «*хідний» може означати «вхідний», «вихідний», «західний». Фраза «?хідний» може означати «вхідний», «східний».

Синтаксис функції: =VLOOKUP(потрібне значення; діапазон; номер стовпця в діапазоні зі значенням, що повертається; TRUE (приблизний збіг) або FALSE (точний збіг)).

Особливість функції – пошук потрібного значення завжди відбувається в першому стовпці вказаного діапазону. Відповідно, значення, які ми можемо отримати, знаходяться в стовпцях праворуч (!) від першого стовпця діапазону. Пошук необхідного значення в першому стовпці діапазону відбувається до першого збігу потрібного значення.

MATCH (ПОИСКПОЗ) – функція повертає номер (відносне положення) комірки в діапазоні (в рядку або в стовпці), значення якої відповідає шуканому критерію.

Синтаксис функції: =MATCH (потрібне значення; діапазон, що переглядається; [тип зіставлення -1, 1 або 0])

INDEX (ИНДЕКС) – функція повертає значення комірки, використовуючи для її пошуку значення зміщення в рядку та стовпці заданого діапазону.

Синтаксис функції: =INDEX(діапазон; номер рядка; [номер стовпця])

Якщо порівнювати комбінацію INDEX+MATCH з функцією VLOOKUP, то треба вказати на певні обмеження останньої, в той час коли вказана комбінація виконує навіть «лівий VLOOKUP».

COUNTA (СЧЁТЗ) – функція повертає число непорожніх комірок у вказаному діапазоні. Приклад: COUNTA(A3:D8). Формула підраховує комірки, що містять числові значення, текст і логічні значення. Якщо в комірці міститься формула, яка повертає порожній рядок, то вона теж рахується, незважаючи на те, що в комірці нічого не відображається.

Синтаксис функції: =COUNTA(діапазон)

COUNT (СЧЁТ) – функція повертає число комірок у вказаному діапазоні, які містять тільки числові значення. Комірки, що містять значення дат і часу, також вважаються числовими. Комірки, що містять логічні значення (FALSE, TRUE), такими не вважаються.

Синтаксис функції: =COUNT(діапазон)

Доволі часто доводиться переносити в різні комірки частини рядка, який записано в одній комірці. Вище вже розглядалося розділення дати і часу за допомогою команди «Текст за стовпцями» (вкладка «Дані»). Наприклад, у комірці записані прізвище, ім'я та по батькові, а потрібно це розбити в різні стовпці, то можна скористатися вказаною командою. Якщо нам потрібна лише одна частина рядка, то використовують формули з текстовими функціями LEFT, RIGHT, FIND, MID. Конструкція таких формул відносно складна, і ми рекомендуємо скористатися макросом.

Спочатку налаштуємо стрічку вкладок команд, додавши на неї вкладку «Розробник». Для цього переходимо на вкладку «Файл», у розділі Параметри > «Налаштування стрічки» у списку панелі «Основні вкладки» встановлюємо прапорець «Розробник».

Відкриваємо редактор Visual Basic на вкладці «Розробник», або тиснемо клавіші <Alt+F11>. Вставляємо новий модуль (меню Insert – Module) і вводимо текст функції:

```
Function ExtractWord(Txt, n) As String
Dim x As Variant
Const DELIM = " "
x = Split (Txt, DELIM)
If n > 0 And n – 1 <= UBound(x) Then
ExtractWord = x(n – 1)
Else
ExtractWord = " "
End If
End Function
```

Потрібно зберегти файл у форматі з підтримкою макросів (XLSM) і повернутися з редактора Visual Basic в Excel.

Синтаксис функції: =ExtractWord(Txt; n), де Txt – адреса комірки з текстом, з якої вибираємо фрагмент тексту; n – порядковий номер фрагмента.

Функцію можна знайти на вкладці «Формули», кнопка «Вставити функцію» у категорії «Визначені користувачем», або в рядку формул кнопка f_x. У діалоговому вікні «Аргументи функції» (рис. 28.27) вказуємо адрес комірки з повним текстом та номер фрагмента (для нашого прикладу це 1, якщо вибирати тільки прізвище). Методом перетягування за маркер заповнення скопіюємо формулу в інші комірки стовпця.

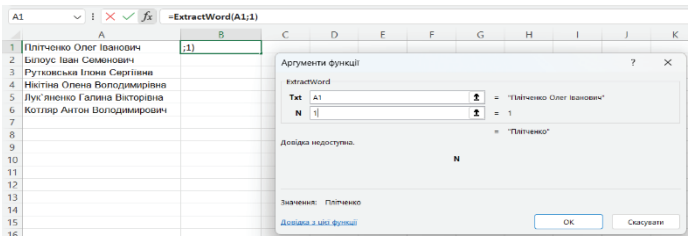


Рисунок 28.27. Вставка функції

Іноді, навпаки, потрібно помістити в одну комірку вміст кількох комірок. Для цього використовують функцію CONCATENATE або символ амперсанда (&).

Якщо на листі розташовано багато комірок, у яких значення отримані за допомогою формул, то при копіюванні та перенесенні цих значень можуть виникати помилки або втрата цих значень. У такому разі потрібно замінити формулу на її значення. Це можна зробити за допомогою команди «Спеціальна вставка», але простіше це зробити за допомогою макроса:

```
Sub Replace_Formulas()
Selection.Copy
Selection.PasteSpecial Paste:=xlValues
End Sub
```

Тепер, якщо виділити на аркуші діапазон комірок (з формулами) і запустити наш макрос (<Alt+F8>, або вкладка «Розробник» > кнопка «Макроси»), то, замість формул у комірках, ми побачимо звичайні значення.

При імпорті даних із різних джерел таблиці можуть містити порожні комірки. Це може погано вплинути на подальші операції форматування, фільтрації або сортування даних. Тобто, порожні комірки треба прибрати (видалити). Робити це вручну не зручно, тому використаємо наступний макрос:

```
Function NoBlanks(DataRange As Range) As Variant()
Dim N As Long
Dim N2 As Long
Dim Rng As Range
Dim MaxCells As Long
Dim Result() As Variant
Dim R As Long
Dim C As Long
MaxCells = Application.WorksheetFunction.Max( _
Application.Caller.Cells.Count, DataRange.Cells.Count)
ReDim Result(1 To MaxCells, 1 To 1)

For Each Rng In DataRange.Cells
If Rng.Value <> vbNullString Then
N = N + 1
Result(N, 1) = Rng.Value
End If
Next Rng
For N2 = N + 1 To MaxCells
Result(N2, 1) = vbNullString
Next N2
If Application.Caller.Rows.Count = 1 Then
NoBlanks = Application.Transpose(Result)
Else
NoBlanks = Result
End If
End Function
```

Порядок роботи з макросом наступний. Виділяємо достатній діапазон комірок деякого стовпця. Вибираємо функцію NoBlanks у категорії «Визначені користувачем». У діалоговому вікні «Аргументи функції» вказуємо вихідний діапазон і тиснемо <Ctrl+Shift+Enter>, щоб ввести функцію як формулу масиву.

Для випадкового вибору записів таблиці (що часто використовують у статистичних розрахунках) скористаємось такою функцією:

```
Function Lotto(Bottom As Integer, Top As Integer, Amount As Integer)
Dim iArr As Variant
Dim i As Integer
Dim r As Integer
Dim temp As Integer
Dim Out(1000) As Variant

Application.Volatile

ReDim iArr(Bottom To Top)
For i = Bottom To Top
iArr(i) = i
Next i
For i = Top To Bottom + 1 Step -1
r = Int(Rnd() * (i - Bottom + 1)) + Bottom
temp = iArr(r)
iArr(r) = iArr(i)
iArr(i) = temp
Next i
j = 0
For i = Bottom To Bottom + Amount - 1
Out(j) = iArr(i)
j = j + 1
Next i

Lotto = Application.Transpose(Out)
End Function
```

Перед тим, як користуватися функцією, потрібно мати стовпець із нумерацією рядків таблиці даних (краще зліва). У діалоговому вікні «Аргументи функції» вказують:
Bottom – нижня межа інтервалу випадкових чисел;
Top – верхня межа інтервалу випадкових чисел;
Amount – кількість випадкових чисел, які ми хочемо відібрати з інтервалу.

Наприклад, щоб відібрати 15 випадкових чисел від 1 до 100, потрібно буде ввести: = Lotto (1; 100; 15).

Звертаємо увагу на те, що функція Lotto має бути введена як формула масиву. Тобто, спочатку необхідно виділити діапазон комірок для результатів, потім ввести функцію Lotto, і після введення аргументів функції, натиснути <Ctrl+Shift+Enter>, щоб ввести цю функцію саме як функцію масиву у всі виділені комірки.

Далі залишається за допомогою функції VLOOKUP витягнути дані з таблиці, які відповідають отриманим випадковим номерам.

Python

Сучасні набори даних містять мільйони записів, і ці набори постійно збільшуються. Для обробки й аналізу великих даних уже недостатньо можливостей Excel. Хоча один лист в Excel має 1 048 576 рядків та 16 384 стовпців (і таких листів в одній книзі Excel можна створити 255), цього недостатньо для ефективної роботи з великими даними. По-перше, якщо дані буде розміщено на сотнях тисяч рядків, Excel буде «гальмувати», швидкість доступу до даних суттєво уповільнюється. Усе ж таки Excel розрахований на обробку невеликих наборів даних і для масштабних обчислень він не підходить. Для розв'язання вказаних проблем використовують мову Python, яка навпаки може *масштабуватися* до обсягу пам'яті комп'ютера й навіть масштабувати обчислення поза пам'яттю пристрою на зовнішньому кластері за допомогою бібліотеки Dask.

Щодо одночасної роботи з декількома джерелами даних різного формату (txt, csv, xlsx, json, sql), то в Excel це можливо за рахунок використання вбудованого редактору **Power Query**. Бібліотеки Python це вирішують значно краще, оскільки не поєднують одночасно й сховище даних, й обчислювальний механізм, на відміну від Excel. Працюючи із зовнішніми джерелами, які змінюються з часом, ми маємо вирішувати задачу *оновлення* даних для оновлення результатів аналізу. Якщо в Excel це робиться більшою мірою вручну, Python дозволяє автоматизувати процес оновлення декількома рядками коду. Приведений порівняльний аналіз вказує на необхідність застосування аналітиками мови Python для обробки та аналізу великих наборів даних.

Треба зауважити, що на даний момент існує бета-версія Microsoft 365, у якій мова програмування Python *інтегрована* в Excel та в Power Query для поліпшення можливості аналізу та візуалізації даних. Це дає можливість виконувати розширений аналіз даних у звичному середовищі Excel, отримуючи доступ до Python безпосередньо зі стрічки Excel. У будь-якому разі залишається необхідним знання тих бібліотек Python, які використовуються для роботи зі структурованими даними, зокрема з електронними таблицями.

Коли ми говоримо про обробку значних обсягів інформації, то маємо на увазі таке поняття, як **Big Data**. Для характеристики великих даних використовують «три V»: їх обсяг (англ. volume), швидкість накопичення нових даних та їх обробки (англ. velocity) і різноманіття типів даних, які можуть оброблятися (англ. variety). Узагалі, до Big Data відносять як структуровані, так і неструктуровані («сирі») дані. Обробка неструктурованої інформації передбачає такий процес: перевірка даних, перетворення до необхідних форматів і *очищення* даних. Цей процес називають інженерією даних.

Заразом із поняттям Big Data існує близьке за значенням і змістом поняття **Data Science** (наука про дані). Традиційний Data Science передбачає поступовий аналіз невеликих пакетів даних, сортування та редагування даних перед аналізом. Отже, спочатку дані збирають, опрацьовують і зберігають, і лише потім аналізують. Щодо Big Data, то є певні відмінності, а саме: дані аналізуються в початковому вигляді і в реальному часі, по мірі їх надходження. У новому підході до роботи з великими даними використовується машинне навчання, для того щоб комп'ютер сам шукав результати опрацьованих даних.

Для обробки й аналізу даних, які, переважно пов'язані з Data Science *Python* використовує відповідні бібліотеки.

Найбільш популярною є бібліотека **Pandas**. Крім читання даних із файлової системи, бібліотека виконує таке: первинний аналіз даних; трансформацію даних (виправлення відсутніх та некоректних значень); вилучення з даних аналітичних показників; запис результатів назад у файлову систему.

Openpyxl – бібліотека використовується для читання, модифікації та запису електронних таблиць. Бібліотека працює з файлами Excel не тільки формату xlsx, а також і формату xlsm, тобто з тими електронними таблицями, які містять макроси. За допомогою модуля openpyex можна відшукувати

в книзі xlsx листи за їх ім'ям або вмістом певних комірок, будувати нові книги, створювати листи в книгах. На відміну від бібліотеки Pandas, модуль openpyxl дозволяє вдатися до низькорівневого програмування на рівні окремих комірок Excel.

NumPy – універсальний і фундаментальний пакет в Python для обробки *масивів* (вектори, матриці тощо)

Бібліотека **SciPy** містить модулі для ефективних математичних процедур, таких як інтерполяція, оптимізація та статистика.

Matplotlib – програмний пакет Python для візуалізації даних із використанням двовимірної і тривимірної графіки. Можна створювати гістограми, стовпцеві, точкові й кругові діаграми. Matplotlib також полегшує використання міток, сіток, легенд та деяких інших об'єктів форматування.

Для роботи з Python необхідно встановити на комп'ютер інтерпретатор Python. Так можна завантажити інсталяційний файл Python з офіційного сайту https://www.python.org/downloads/windows/ і виконати установку (рис. 28.28).



Рисунок 28.28. Встановлення на комп'ютер інтерпретатора Python

Для повноцінної роботи з інтерпретатором додатково встановлюють редактор коду (наприклад, PyCharm), який дозволяє писати програми, зберігати у файли та запускати їх. Узагалі, такі редактори називають інтегрованим середовищем розробки (IDE). Можна об'єднати всі зусилля по встановленню інтерпретатора, пошуку редактору коду, встановленню додаткових модулів і бібліотек, якщо встановити пакет **Anaconda** – дистрибутиви Python (рис. 28.29). Цей пакет надає все необхідне для вирішення завдань щодо аналізу та обробки даних.

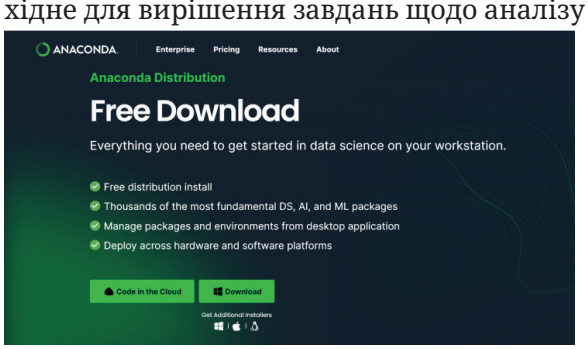


Рисунок 28.29. Встановлення пакету Anaconda

До пакету Anaconda входить Anaconda Navigator – графічний інтерфейс користувача, який дозволяє запускати пов'язані програми та керувати пакетами. У Навігаторі за замовчуванням доступні такі програми, як Jupyter Notebook та Spyder. Зокрема, **Spyder** і є кросплатформове інтерактивне IDE для програмування мовою Python.

Робоче вікно редактора Spyder розділено на дві панелі. В одній панелі розміщують скрипти, а в іншій панелі проглядають результати виконання коду. Друга панель фактично є вбудованою консоллю (IPython console), у якій, крім виводу виконання коду, можна виконувати різні скрипти (команди). Наприклад, отримати довідку для команди pip, яка призначена для встановлення та управління різними пакетами та бібліотеками Python.

Однією з цікавих особливостей Spyder є можливість перегляду значень змінних. У процесі виконання програми змінні виводяться на панелі Variable Explorer у вигляді списку з інформацією про ім'я, тип, розмір і значення змінної. Узагалі, Spyder має унікальне поєднання можливостей – просунуте редагування, аналіз та глибока інспекція коду, гарна візуалізація.

Існують певні правила (синтаксис) написання коду в Python, які треба засвоїти, перед тим, як переходити до програмування й роботи з відповідними бібліотеками:

- *оператором присвоювання значень змінним є знак «=»;*
- *кінець рядка є кінцем інструкції (прикінцеві символи непотрібні);*
- *кілька інструкцій (операторів) в одному рядку розділяють крапкою з комою;*
- *записуючи одну інструкцію в декілька рядків, використовують дужки (круглі, квадратні або фігурні).*
- *якщо є основна інструкція та вкладені до неї інструкції, то основна інструкція завершується двокрапкою, а вкладені інструкції розташовують у нових рядках з однаковим відступом (як мінімум 4 пробіли) від початку рядків по відношенню до основної інструкції. Якщо тіло вкладеної інструкції містить єдиний оператор, то його можна записати в тому ж рядку, що й основна інструкція;*
- *на початку нового рядка, або в рядку в кінці інструкцій можна розміщувати коментар після символу #.*

Щодо вибору ідентифікаторів для змінних, то першим символом може бути буква з алфавіту або символ підкреслення «_». Інша частина ідентифікатора може складатися з букв, символу підкрес-

лення або цифр. Python чутливий до регістру букв в іменах змінних, функцій, операторів, класів (великі і маленькі літери вважаються різними).

Базовими елементами мови Python є структури даних (рядки, списки, діапазони, кортежі, множини, словники), логічні вирази й логічні оператори, оператори розгалуження та цикли. Якщо в програмі використовують якісь модулі (бібліотеки), то потрібно це вказати за допомогою інструкції import. Для отримання практичних навичок базового програмування на мові Python існує багато різних джерел в інтернеті та безкоштовних онлайн-курсів.

Аналіз даних у Python продемонструємо на прикладі таблиці банківських транзакцій. Будемо вважати, що таблиця розміщена у файлі Excel та має таку структуру:

поле "id" - номер (або назва) рядків, формат даних – числовий або текстовий;

поля "Джерело" і "Призначення" – номери банківських рахунків, формат даних – текстовий;

"Дата" – дата транзакції, формат даних – дата (dd.mm.yy);

"Час" – час транзакції, формат даних – час (h:mm:ss);

"Сума коштів" – сума транзакції (формат даних – числовий).

Аналіз таблиці банківських транзакцій може передбачати обчислення наступних показників:

- *кількість транзакцій загальна;*
- *кількість транзакцій з кожного рахунку;*
- *рахунок, з якого приходиться найбільша кількість транзакцій;*
- *кількість транзакцій на певний рахунок (або певні рахунки);*
- *рахунок, на який приходиться найбільша кількість транзакцій;*
- *кількість транзакцій за конкретну дату (або певний термін);*
- *дата, на яку прийшлася найбільша кількість транзакцій;*
- *загальна сума коштів для всіх транзакцій;*
- *сума коштів для транзакцій із певного рахунку (або певних рахунків);*
- *сума коштів для транзакцій за конкретну дату (або певний термін);*
- *максимальний (мінімальний) переказ;*
- *рахунок, з якого (або на який) надійшла найбільша (найменша) сума коштів.*

Аналіз таблиці банківських транзакцій із використання бібліотеки Pandas.

Почнемо з команд імпорту необхідних бібліотек:

```
import pandas as pd
import numpy as np
```

Далі, потрібно завантажити дані з Excel у Python. Це виконає функція pd.read_excel. Повний синтаксис функції імпорту в нашому прикладі (рис. 28.30):

```
banktr = pd.read_excel('banktransactions.xlsx', sheet_name = 'початкова', index_col = 'id', dtype = str)
```

Вводимо ідентифікатор banktr, якому привласнюємо об'єкт датафрейм бібліотеки Pandas. Фактично, це і є таблиця банківських транзакцій з усіма її стовпцями і рядками, але тепер до неї може бути застосований великий набір функцій бібліотеки Pandas. Перші два параметри функції обов'язкові – ім'я файлу та ім'я листа. Можна імпортувати таблицю без рядка заголовку (header=None) або окремі стовпці таблиці (usecols=['ім'я_стовпця', 'ім'я_стовпця']). Якщо вихідна таблиця в Excel має стовпець із назвами або номери рядків, то в параметрі index_col вказуємо його ім'я. Як правило, такий стовпець називають лічильником або автонумерацією, і він наявний у таблицях баз даних (у таблицях Excel це є не завжди). Однак, якщо ми будемо виконувати сортування або фільтрацію даних у таблиці, то, щоб повернути її до вихідного вигляду, допоможе

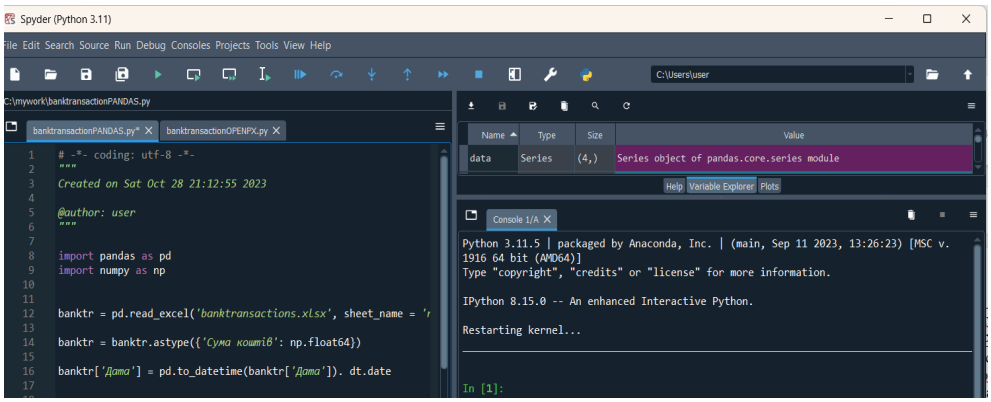


Рисунок 28.30 Початок роботи в Python

лічильник. Ще одна особливість лічильника: при видаленні певних рядків із таблиці їх номери видаляються назавжди і вже не будуть зустрічатись знову.

Серед параметрів функції імпорту ми бачимо параметр dtype. У нашому прикладі цей параметр приймає значення str. Це означає, що всі дані будуть імпортовані в текстовому форматі, навіть і ті, які за змістом числові. Це має певний сенс, оскільки, по-перше, імпортування в такому разі відбувається значно швидше, а по-друге, ми не втратимо частину інформації. Зокрема, якщо номер рахунку починається з нуля (наприклад, '05889431715'), то при імпортуванні без вказаного параметра Pandas відкине нуль і зробить номер рахунку звичайним числом. Дані стовпця «Сума коштів» теж будуть мати текстовий формат, але це можна виправити, якщо застосувати функцію зміни формату astype(). Команда така: banktr = banktr.astype({'Сума коштів': np.float64})

Зауважимо, що float64 – це числовий тип даних Pandas. До речі, текстовий тип даних Pandas позначається як object.

Отже, можемо сказати, що перший крок роботи з даними в Python зроблено – перевірка даних і перетворення до необхідних форматів.

Наступним кроком проглянемо деякі властивості набору даних.

Команда	Параметр, який повертає команда
len(banktr)	кількість рядків таблиці
banktr.shape	кількість рядків і кількість стовпців, пара значень (n_rows, n_columns)
banktr.columns	заголовок таблиці (список із назв стовпців)
banktr.head()	перші п'ять рядків датафрейма
banktr.sample()	п'ять випадкових записів датафрейма
banktr.index	назви (номери) рядків таблиці, ім'я стовпця автонумерації і кількість номерів
banktr.describe()	статистичні відомості датафрейма: середнє, мінімальне, максимальне значення і т.ін. у стопці з числовими даними
banktr.info()	відомості про датафрейм: кількість записів, кількість стовпців, заголовки стовпців, формат даних у стовпцях, окремо кількість стовпців текстового, числового форматів, об'єм пам'яті, що використовує датафрейм
len(banktr['Джерело'].unique())	кількість унікальних значень у стовпці

Повернемось до аналізу даних таблиці банківських транзакцій. Загальна кількість транзакцій може бути знайдена за допомогою команд len(banktr), banktr.shape, banktr.info().

Задачу підрахунку кількості транзакцій з кожного рахунку можна вирішити за допомогою команди banktr.groupby('Джерело')['Сума коштів'].count()

Тобто, ми отримаємо зведену таблицю з двох стовпців – номери рахунків та кількість транзакцій по кожному рахунку. Однак, краще мати цю таблицю, яка відсортована по кількості транзакцій. Це вирішить команда

banktr.groupby(['Джерело'])['Сума коштів'].agg(['count']).sort_values(by ='count', ascending=False).head(10)

Отже, відразу бачимо рахунок, з якого надходить найбільша кількість транзакцій. Команда надає 10 записів, що вказано в методі .head.

Для підрахунку кількості транзакцій на певний рахунок (або певні рахунки) та визначення рахунку, на який приходиться найбільша кількість транзакцій, використовуємо ту ж саму конструкцію, замінивши назву стовпця «Джерело» на «Призначення».

Для підрахунку кількості транзакцій на конкретну дату та визначення дати, на яку прийшлася найбільша кількість транзакцій, використовуємо ту ж саму конструкцію, замінивши назву стовпця «Джерело» на «Дата».

Загальну суму коштів для всіх транзакцій можна знайти так:

banktr['Сума коштів'].sum()

Сума коштів для всіх транзакцій з певного рахунку (або певних рахунків) підраховується шляхом складання фільтру:

filter_source = banktr['Джерело'] == '01223854840'

та фільтрації датафрейму: D1 = banktr.loc[filter_source]

Ми отримаємо новий датафрейм D1, до якого знову застосуємо конструкцію ["Сума коштів"].sum(): banktr.loc[filter_source]['Сума коштів'].sum()

Щоб отримати рахунок, з якого надійшла найбільша сума коштів, застосуємо команду: banktr.groupby(['Джерело'])['Сума коштів'].agg(['sum']).sort_values(by='sum', ascending=False).head(10)

Ми бачимо схожу конструкцію з підрахунку кількості транзакцій, тільки метод count замінено на sum. До речі, якщо ми хочемо бачити рахунок, з якого надійшла найменша сума коштів, сортувати треба у зворотньому порядку, тобто призначити ascending=True. Якщо до того ж потрібно проглянути, на які дати приходились певні сумарні перекази з рахунків, застосуємо таку команду:

banktr.groupby(['Джерело', 'Дата'])['Сума коштів'].agg (['sum']).sort_values(by ='sum', ascending=False).head(10)

Тобто, додали групування по стовпцю «Дата» (рис. 28.31).

Для отримання максимального переказу можна стовпець «Сума коштів» перетворити в список List1 = banktr['Сума коштів'].tolist() та застосувати функцію max

max(List1)

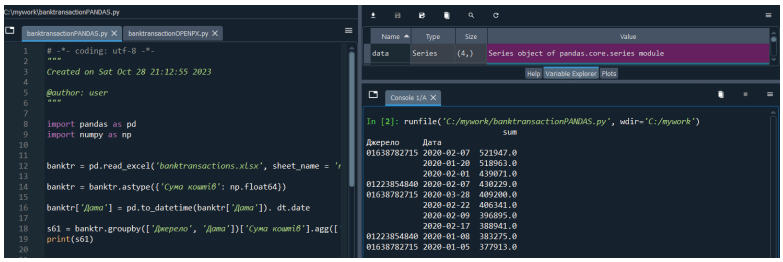


Рисунок 28.31. Групування по стовпцю «Дата»

Але якщо ми хочемо побачити не тільки максимальний переказ, а ще й рахунок, з якого цей переказ надійшов, краще створити новий датафрейм тільки з двох стовпців df1 = banktr[['Джерело', 'Сума коштів']] і, потім виконати сортування df1.sort_values('Сума коштів', ascending=False)

Закінчуючи аналіз таблиці банківських транзакцій (з наведених показників) за допомогою бібліотеки Pandas, можна впевнено сказати, що її можливості не тільки повторюють, але й перевершують можливості Excel.

Аналіз таблиці банківських транзакцій із використання бібліотеки Openpyex.

Код в Python починається з підключення необхідних модулів:

```
from openpyxl import load_workbook, Workbook
import matplotlib as mpl
import matplotlib.pyplot as plt
```

Відкриємо файл xlsx в Python:

```
wb = load_workbook(filename = 'banktransactions.xlsx', data_only=True, read_only=True)
```

Функція load_workbook() приймає ім'я файлу як аргумент та повертає об'єкт робочої книги, який представляє файл. Це можна перевірити за допомогою команди type (wb). У даному випадку в команді ми не вказуємо повний шлях до файлу xlsx, маючи на увазі, що файл розташовано в робочій директорії, тобто робочій простір було підготовлено заздалегідь. Файл xlsx відкривається лише для читання, на що вказує атрибут read_only зі значенням True.

Якщо зчитувані дані з Excel містять формули, то інструкція data_only = True дозволить завантажити лише значення комірок.

Для того щоб позиціонуватися на першому листі книги xlsx (яких у книзі може бути декілька), потрібно в об'єкті wb визвати метод active: sheet = wb.active

Нумерація листів починається з 0 (і не залежить від ім'я листа). Якщо нам буде потрібно зробити активним другий лист книги, то команда така:

```
wb.active = 3
sheet = wb.active
```

Для того щоб звернутися до вмісту окремих комірок листа, використовують метод value об'єкта sheet, а саме: sheet['A1'].value, або sheet[1][0].value (стиль R1C1).

Зауважимо, що для відносних посилань на комірки, нумерація стовпців починається з нуля (тобто, стовпець А позначено як 0, В – як 1, С – як 2 і т.ін.).

Якщо ми хочемо переглянути всі рядки (або їх частину) таблиці банківських транзакцій, то можна побудувати цикл:

```
for row in range(1, sheet.max_row+1):
        print(sheet['A'+str(i)].value, sheet['B'+str(i)].value,
  sheet['C'+str(i)].value, sheet['D'+str(i)].value)
```

Зауважимо, що параметр циклу row є зарезервованою змінною. Конструкція sheet.max_row повертає кількість заповнених рядків таблиці. Оскільки range «не бере» останнє значення циклу, то потрібно додати одиницю.

Для того щоб вибрати та переглянути дані з певного діапазону таблиці, використовують конструкцію:

```
cells = sheet['B1':'C11']
for Призначення, Дата in cells:
print(Призначення.value, Дата.value)
```

Якщо нам потрібно звернутися до певної комірки листа книги, то це можна зробити такою конструкцією:

```
sheets = wb.worksheets
print(sheets[0]['B2'].value) # перший лист
```

Змінна sheets є список назв листів, як об’єктів, для можливості звертатися до комірок цих листів.

Можна проглянути список листів робочої книги:

```
wsn = list(wb.sheetnames)
print(wsn)
```

Іноді в робочій книзі потрібно знайти саме той лист (коли їх декілька), який містить необхідну нам інформацію. Якщо ознакою цього листа є певний текст у відомій нам комірці, то це вирішується за допомогою циклу:

```
wsdate = None
    for i in wsn:
        if wb[i]['B1'].value == 'Джерело':
            wsdate = i
```

У даному випадку ми шукаємо лист, у якому в комірці В1 зберігається текст «Джерело». За умови, коли такого листа не знайдеться, краще додати таку конструкцію:

```
if wsdate == None:
raise NotAllData('Нема такого листа')
```

Коли необхідний лист знайдено, треба створити об’єкт-лист для подальшої роботи з атрибутами цього об’єкту: ws = wb[wsdate]

Подальший код створює список із назв стовпців вихідної таблиці:agolovok = [cell.value for cell in next(ws.iter_rows(min_row=1, min_col=1, max_row=1, max_col=ws.max_column))]

Далі створимо словник, який збирає для кожного рахунку-відправника (це ключ словника) всю іншу інформацію, тобто всі рахунки-отримувачі, дату, час і суму перерахованих коштів (це значення словника).

Для початку створюється порожній словник: pryznachdata = {}.

У наступному фрагменті коду словник pryznachdata заповнюється елементами. Цикл пробігає всі рядки таблиці (починаючи з другого) і для рахунку-відправника (змінна priz) збирає дані, формуючи список із даних рядків (змінна prizdata). Спочатку перевіряється, чи не є наступний рядок порожнім. Якщо ні, то формується ключ словника, як значення комірки першого стовпця та поточного рядка. Оскільки номери рахунків у першому стовпці таблиці можуть повторюватися, то для кожного такого рахунку, який уперше потравляє як ключ до словника, створюється порожній список prizdata.

```
for row in ws.iter_rows(min_row=2, min_col=1, max_row = ws.max_row, max_col=ws.max_column):
    if len(row) > 0:
        priz = row[1].value
        if priz is not None:
            prizdata = [cell.value for cell in row]
            if priz not in pryznachdata:
                pryznachdata[priz] = []
            pryznachdata[priz].append(prizdata)
```

Наявність побудованого словника дозволяє дати відповідь на питання, з якого рахунку надійшла найбільша (найменша) сума коштів. Для цього створимо такий словник: dicprizsum = {}.

```
for priz in pryznachdata:
    dicprizsumka[priz] = 0
    for i in range(len(pryznachdata[priz])):
        dicprizsumka[priz] = dicprizsumka[priz] + pryznachdata[priz][i][5]
    print("З рахунку", priz, "перераховано", dicprizsumka[priz])
```

У коді створення словника маємо зовнішній цикл, який «пробігає» ключі словника pryznachdata, та внутрішній – по кожному рядку значення ключа, звертаючись саме до перерахованих сум і кожного разу накопичуючи суму переказів. Елементи рядка (як списку) рахуються з 0, тому сума коштів у рядку рід номером «і» – це pryznachdata[priz][i][5].

Отже, проглядаючи результати коду, можна отримати, з якого рахунку на інші рахунки надійшла найбільша (найменша) сума коштів. Узагалі, таких рахунків може бути досить багато, і візуально знайти найбільшу суму буде складно, але це швидко можна визначити. Використовуючи словник dicprizsum, створимо список зі значень сум та застосуємо до нього метод max.

```
valuesListSum = list(dicprizsumka.values())
print('Найбільша перерахована сума складає', max(valuesListSum))
```

До того ж, використовуючи цикл за ключем у словнику, можна вказати і сам рахунок, з якого надійшла найбільша сума коштів:

```
for priz in dicprizsumka:
    if max(valuesListSum)==dicprizsumka[priz]:
        print("Рахунок, з якого надійшла найбільша сума - це ", priz)
```

Кількість транзакцій із кожного рахунку визначимо за допомогою циклу за ключем у словнику pryznachdata та методом len (довжина), який застосовується до списку значень ключа pryznachdata[priz].

```
chika = {}
for priz in pryznachdata:
    chika[priz]=len(pryznachdata[priz])
for priz in pryznachdata:
    print("З рахунку", priz, "відбулося транзакцій", len(pryznachdata[priz]))
```

Наступна задача продемонструє більш помітні можливості Python для роботи з Excel. Оскільки більшість питань з аналізу таблиці банківських транзакцій відноситься до окремих рахунків, то було би значно простіше, коли дані для певного рахунку були б розташовані на окремому листі книги Excel або в окремій книзі. Отже, засобами Excel створимо нові книги окремо для кожного рахунка-відправника. Зрозуміло, що в кожній такій книзі будуть зібрані записи з основної таблиці тільки для певного рахунку.

Спочатку треба закрити поточну книгу-об'єкт: wb.close. У наступному коді створюються книги окремо для кожного рахунка-відправника.

```
for priz in pryznachdata:
wb = Workbook()
ws = wb.active; ws.title = "Рахунок " + priz
ws.append(zagolovok)
for row in pryznachdata[priz]:
    ws.append(row)
exfilname = join('.', 'Result', (priz + '.xlsx'))
exfilname = abspath(exfilname)
wb.save(exfilname)
wb.close
```

Як ми бачимо, знову став у пригоді словник pryznachdata. Для кожного окремого рахунка-відправника ми створюємо нову книгу-об'єкт, вказуємо назву листа, формуємо на листі заголовок таблиці та додаємо на лист інші записи (значення ключа словника). Далі формуємо ім'я файлу (з указанням ім'я директорії, у яку будуть записані всі файли), зберігаємо його на диск і закриваємо об'єкт книга поточного елементу циклу.

Інтерактивна візуальна аналітика в Python.

Розглянемо побудову карти розташування базових станцій мобільного зв'язку з таблиці трафіку з'єднань засобами Python. Для цього використаємо бібліотеку (модуль) folium.

Folium – це потужна бібліотека візуалізації геопросторових даних у Python. За допомогою folium можна створити інтерактивну карту будь-якого розташування у світі, якщо ми знаємо його значення широти та довготи. Також можна на карту накласти маркери та кластери маркерів.

Перед тим, як безпосередньо використати модуль folium, потрібно підготувати список координат. У наступному коді ми створюємо об'єкт книгу, відкриваючи файл trafik.xlsx, робимо активним перший лист, формуємо список координат (список coordata) та видаляємо дублікати координат (список coordwd). Зауважимо, що стовпець координат у таблиці трафіку з'єднань (у нашому прикладі) починається з 7-го стовпця.

```
import folium
from folium.plugins import MarkerCluster
from folium.plugins import MousePosition
from folium.features import DivIcon

import os
from openpyxl import load_workbook, Workbook
from openpyxl.styles import Alignment, PatternFill, Font
from os.path import join, abspath
from math import *

class NotAllData(Exception):
    pass

os.chdir("C:/Mywork/")

def toFixed(numObj, digits=0):
    return f"{numObj:.{digits}f}"

wb = load_workbook(filename = "Traffic.xlsx", data_only=True, read_only=True)
ws = wb.active

coordata = []
for row in ws.iter_rows(min_row=2, min_col=7, max_row=ws.max_row, max_col=ws.max_column):
    cdata = [cell.value for cell in row]
    coordata.append(cdata)

coordwd = []
[coordwd.append(x) for x in coordata if x not in coordwd]
```

Далі необхідно визначитися з координатами того району, який охоплює базові станції, координати яких приведено у вихідній таблиці і які будуть нанесені на карту цього району у вигляді маркерів. Для цього зробимо таке:

```
coordwd0 = []
for x in coordwd:
    coordwd0.append(x[0])
coordwd1 = []
for x in coordwd:
    coordwd1.append(x[1])

minlat = min(coordwd0)
maxlat = max(coordwd0)
latR = toFixed((minlat + maxlat)/2, 2)
minlong = min(coordwd1)
maxlong = max(coordwd1)
longR = toFixed((minlong + maxlong)/2, 2)
```

У цьому коді ми спочатку створюємо два списки. Список coordwd0 утворено зі значень широти, які ми отримали в списку coordwd, а список coordwd1 утворено зі значень довготи. У кожному з цих списків ми знаходимо мінімальне та максимальне значення, та їх середнє арифметичне (latR і longR). І ще, у значеннях latR та longR ми залишаємо тільки два десяткових знаки. Це робить функція toFixed.

Тепер ми маємо пару [latR, longR], яку використаємо в головному рядку коду, що фактично створює карту:

```
map = folium.Map(location=[latR,longR], tiles='openstreetmap',zoom_start = 13)
```

Параметр tiles використовують для зміни фону (або стилю) картки. Узагалі, існують три стиля карт. Стиль карти за замовчуванням – OpenStreetMap (відкрита карта вулиць), яка показує вигляд та назву вулиць та межі країн світу. Стиль Stamen Toner дозволяє отримувати висококонтрастні чорно-білі карти. Цей стиль підходить для візуалізації та вивчення річкових меандрів (вигини русла річки) та

прибережних зон. Стиль Stamen Terrain (тиснення місцевості) підходить для візуалізації затінення пагорбів та природних кольорів рослинності.

Параметрzoom start – це початковий рівень масштабування, який після відображення карти можна легко змінити шляхом збільшення або зменшення масштабу.

Перейдемо до нанесення маркерів (позначок станцій) на карту.

```
for coordinates in coordwd:
folium.Marker(location=coordinates, icon=folium.Icon(color = 'blue')). add_to(map)
```

Як бачимо, маркери утворюються за допомогою методу Marker з параметрами location та icon. Ці параметри визначають координати маркерів та їх колір. Саме тут нам знадобився список coordwd.

За допомогою наступного коду можна бачити координати будь-якої точки на карті при наведені на неї курсора миші. Це невеличке вікно, яке може бути розташовано, наприклад, зверху в правому куті карти - topright.

```
formatter = "function(num) {return L.Util.formatNum(num, 5);};"
mouse_position = MousePosition(
    position ='topright',
    separator ='Long: ',
    empty_string ='NaN',
    lng_first = False,
    num_digits = 20,
    prefix = 'Lat:',
    lat_formatter = formatter,
    lng_formatter = formatter
)
map.add_child(mouse_position)
```

Нарешті, побудовану карту зберігаємо у файлі html для подальшого її перегляду з браузера: map.save(«My_map1.html») (рис. 28.32)

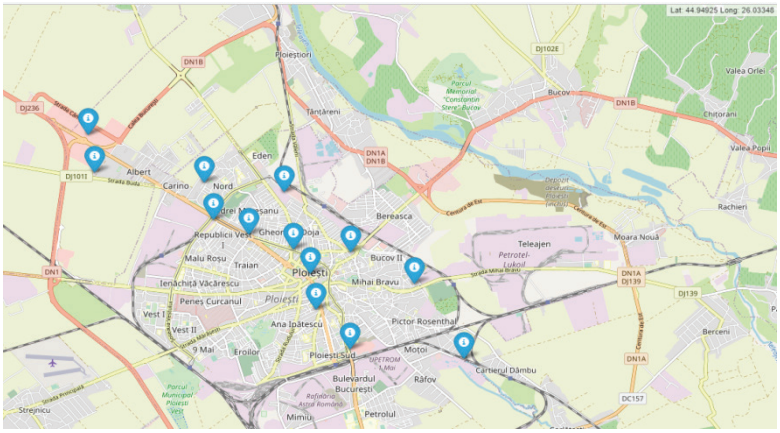


Рисунок 28.32. Побудова карти в Python

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Джонстоун Дженніфер, Яніцкі Мірослав, Навроцкі Даріуш. Посібник з кримінального аналізу для кримінальних аналітиків Державної прикордонної служби України. Київ: ОБСЄ, 2015. 178 с.
2. Костюченко А.О. Основи програмування мовою Python: навчальний посібник. Чернігів: ФОП Баликіна С.М., 2020. 180 с.
3. Нелюбов В.О., Куруца О.С. Основи інформатики. Microsoft Excel 2016: навчальний посібник. Ужгород: ДВНЗ «УжНУ», 2018. 58 с.
4. Основи кримінального аналізу: посіб. з елементами тренінгу / Користін О.Є., Албул С.В., Холостенко А.В. та ін. Одеса: ОДУВС, 2016. 112 с.
5. Федчак І. А. Основи кримінального аналізу: навчальний посібник. Львів: Львівський державний університет внутрішніх справ, 2021. 288 с.
6. Ґвідо ван Россум, Фред Л. Дрейк. Підручник мови Python. Пер. Сергій Кузьменко. URL: https://uk.wikibooks.org/wiki/Підручник_мови_Python.
7. Підручник з основ Microsoft Excel - Навчання використання Excel. URL: https://websetnet.net/uk/microsoft-excel-basics-tutorial-learning-how-to-use-excel/.
8. Anaconda Distribution. URL: https://www.anaconda.com/products/ distribution.
9. Anaconda Documentation. URL: https://docs.anaconda.com/.
10. IBM i2 Analyst's Notebook. User Help. URL: https://www.ibm.com/docs/ en/SSJSV9_9.2.1/com.ibm.i2.anb.doc/analysts_notebook_pdf.pdf.

DOI: https://doi.org/10.36486/978-966-2310-66-5-29

З приводу ліквідації крейсера «Москва»: спершу було слово (спершу завжди буває слово), і це було слово українського прикордонника. Слово поширилося по всій землі – і через 6 тижнів рускій воєнний корабль прибув на місце, по слову черкащанина.

Оксана Забужко

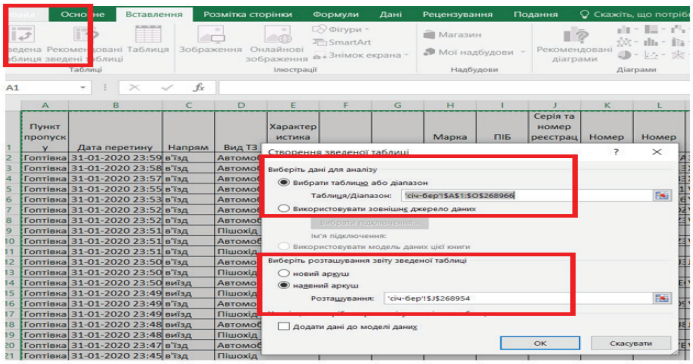
РОЗДІЛ 29
Основні алгоритми роботи аналітика з i2 Analyst's Notebook та Microsoft Excel

Юрій Крутік

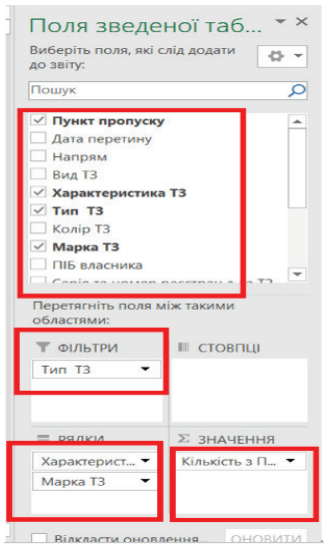
АНАЛІЗ ПЕРЕТИНУ ДЕРЖАВНОГО КОРДОНУ ОСОБАМИ ТА ТРАНСПОРТНИМИ ЗАСОБАМИ

Для відпрацювання аналізу щодо осіб чи транспортних засобів, які часто перетинали державний кордон України протягом певного періоду часу (декілька днів чи декілька років) необхідно:

1. Сформувати відповідний масив даних.
2. Виділити таблицю з вихідними даними, на панелі вкладок перейти до розділу «Вставлення» і обрати кнопку «Зведена таблиця».

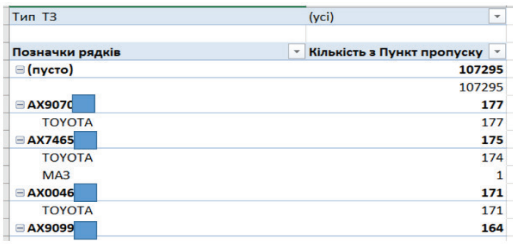


3. Налаштування параметрів вікна, що з'явиться («Створення зведеної таблиці») залишити без змін і натиснути кнопку «ОК».

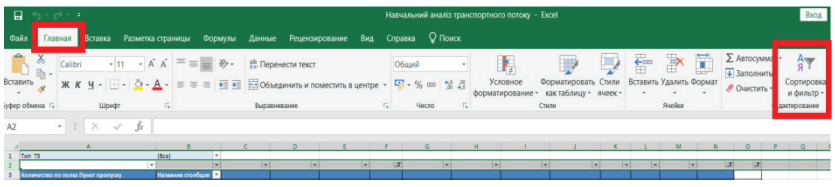


4. Налаштувати поля зведеної таблиці, шляхом перетягування потрібних назв колонок (вихідної таблиці) до областей «Фільтри», «Стовпці», «Рядки», «Значення».

5. При умові здійснення налаштування полів зведеної таблиці вищевказаним чином отримаємо таблицю в якій буде підраховано кількість перетинів кордону транспортними засобами (особами) в пункті пропуску за певний проміжок часу.



Тип ТЗ	(усі)
Позначки рядків	Кількість з Пункт пропуску
(пусто)	107295
	107295
AX907C	177
TOYOTA	177
AX7465	175
TOYOTA	174
MA3	1
AX0046	171
TOYOTA	171
AX9099	164



6. Для відокремлення транспортних засобів (осіб) щодо яких доцільно провести додаткові перевірочні заходи використовуємо кнопку «Сортування і фільтр» розділу «Основне» на панелі вкладок.

7. Перевірити встановлені транспортні засоби та осіб, що у них слідують по наявних обліках (реєстрах), з приводу можливої причетності до здійснення протиправної діяльності.
8. У звіті (висновку) офіцера підрозділу кримінального аналізу вказати про доцільність здійснення додаткових перевірочних заходів із залученням сил та засобів оперативних підрозділів або підрозділів охорони кордону з зазначенням терміну представлення їх результатів.

Якщо потрібно визначити динаміку перетину кордону осіб чи транспортних засобів під певні зміни персоналу Державної прикордонної служби України або інших контрольних служб необхідно освоїти використання окремих функцій програмного забезпечення Microsoft Excel, які використовуються при формуванні вихідного масиву даних, а саме:

Функція «Час» - забезпечує визначення часу, як цілого числа в інтервалі від 0 до 23. *Зразок використання формули =ЧАС(С2).*

Функція «И» - одна з логічних функцій, за допомогою якої можна визначити чи всі умови, що перевіряються, приймають значення істина. Дуже часто при вирішенні різного роду задач функція «И» застосовується разом із функцією «ЕСЛИ».

Функція «Если» дозволяє виконувати логічні порівняння значень і формувати задані результати. У функції «ЕСЛИ» можливі два результати. Перший результат формується, якщо порівняння істинно, другий – якщо порівняння помилкове. *Зразок використання формули*

=ЕСЛИ(И(Н2>=0; Н2<8);1;ЕСЛИ(И(Н2>=8;Н2<20);2;3))

Функція «ВПР» використовується, якщо потрібно знайти елементи в таблиці або діапазоні по рядках. Будемо застосовувати разом із функцією «Если» для автоматичного проставлення у витяг із перетинами кордону т/з умовного номеру зміни Державної прикордонної служби України, залежно від дати і періоду часу. Формула будується наступним чином = ВПР (пошукове значення; таблиця; порядковий номер стовпчика; приблизне або точне співпадіння (1 або 0 відповідно)).

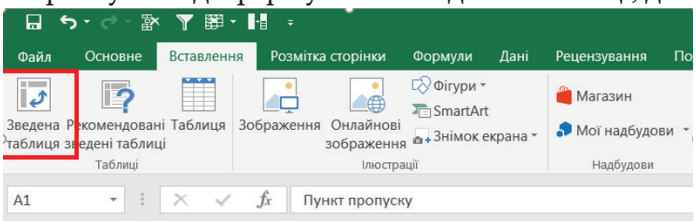
Зразок використання формули

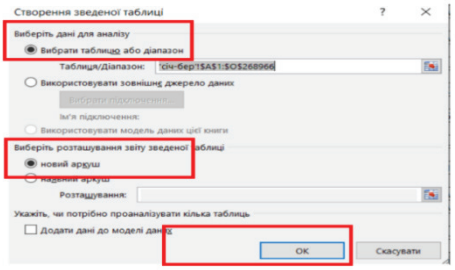
=ЕСЛИ(I2=1;ВПР(B2;$R$15:$Y$44;3;0);ЕСЛИ(I2=2; ВПР(B2;$R$15:$Y$44;5;0; ВПР(B2;$R$15:$Y$44;7;0)))

Посилання на діапазон таблиці має бути абсолютним (не міняється при копіюванні, виділяється знаками $, після натискання клавіші F4).

Після сформування вихідного масиву даних, в якому напроти кожного факту перетину кордону особою (транспортним засобом) буде вказано умовний номер зміни Державної прикордонної служби України (інших контрольних служб), можемо приступати до формування зведеної таблиці, для чого необхідно:

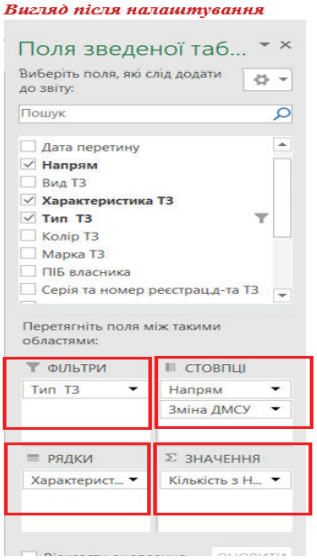
1. Виділити таблицю з вихідними даними, на панелі вкладок перейти до розділу «Вставлення» і обрати кнопку «Зведена таблиця».

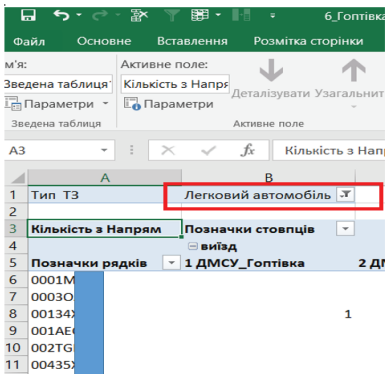




2. Налаштування параметрів вікна, що з'явиться («Створення зведеної таблиці») залишити без змін і натиснути кнопку «ОК».

Вигляд після налаштування

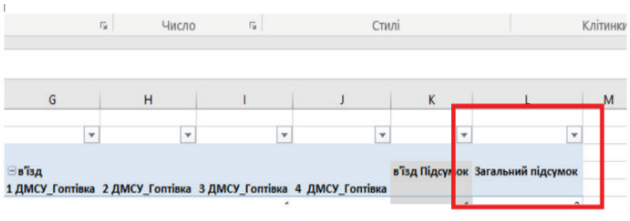




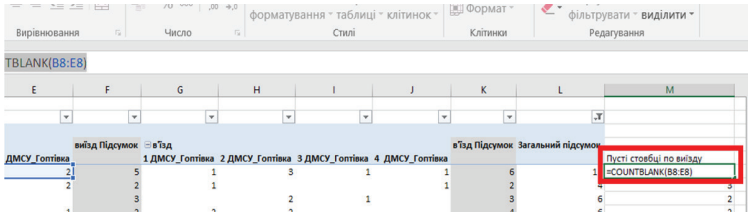
3. Налаштувати поля зведеної таблиці, шляхом перетягування потрібних назв колонок (вихідної таблиці) до областей «Фільтри», «Стовпці», «Рядки», «Значення».

4. При необхідності можна застосовувати фільтр за типом транспортного засобу. Для цього в строчці «Тип ТЗ» необхідно обрати потрібну категорію авто.

5. Виставляємо фільтр в стовпці загальний підсумок, або в стовпцях із узагальненою кількістю перетинів по напрямах слідування, задаємо загальну кількість перетинів кордону відносно кожного автомобіля, які будемо дальше аналізувати.



6. У крайньому пустому правому стовпчику прописуємо формулу підрахунку пустих клітинок розділу таблиці, який стосується напряму слідування - виїзд (якщо в пункті пропуску несуть службу чотири зміни, а підрахунок пустих клітинок покаже значення три, то це буде означати, що відповідний транспортний засіб перетинав кордон виключно під одну зміну персоналу Державної прикордонної служби України). *Зразок використання формули* =COUNTBLANK (B8:E8) .



7. Вигляд таблиці з результатами аналізу авто, які слідували на виїзд з України виключно під одну зміну персоналу Державної митної служби України.

Тип ТЗ	(Все)										
Количество по полю Пу	Назва										
	виїзд				виїзд Итог	в'їзд				в'їзд Итог	Общий итог	Пусті кл. виїзд
Названия строк	1 ДМСУ	2 ДМСУ	3 ДМСУ	4 ДМСУ_Ягодин		1 ДМСУ_	2 ДМСУ_	3 ДМСУ_	4 ДМСУ_Ягодин			
AA2824XB				4	4		1	2		3	7	3
AC8846CK	4				4	1				1	5	3
BC2882EP	7				7		2	6		8	15	3
BC6444AK				4	4	1	1	1	1	4	8	3
BC8498HI		4			4		1			1	5	3
BC9409HI				4	4			1	1	2	6	3
BO4466BC			5		5		1			1	6	3
Общий итог	5023	4878	4939	5157	19997	5774	5053	5842	5395	22064	42061	

8. Аналогічні дії провести для встановлення авто, які слідували на в'їзд в Україну виключно під одну зміну персоналу Державної прикордонної служби України (інших органів влади).

9. Перевірити встановлені транспортні засоби та осіб, що у них слідують по наявних обліках (реєстрах), з приводу можливої причетності до здійснення протиправної діяльності.

10. У звіті (висновку) офіцера підрозділу кримінального аналізу вказати про доцільність здійснення додаткових перевірочних заходів із залученням сил та засобів оперативних підрозділів або підрозділів охорони кордону з зазначенням терміну представлення їх результатів.

Аналіз в'їзду на територію України іноземців та осіб без громадянства.

У ході проведення заходів із протидії нелегальній міграції, офіцер підрозділу, що здійснює кримінальний аналіз може здійснити аналітичне дослідження, за результатами якого встановити списки іноземців та осіб без громадянства, які законно в'їхали на територію України та в подальшому можливо незаконно перетнули державний кордон України чи можливо порушили міграційне законодавство України. Для проведення відповідного кримінального аналізу необхідно:

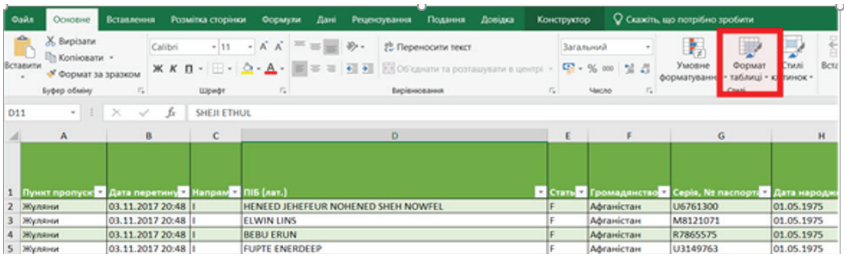
1. Сформувати інформаційні масиви (за період від 1 до 5 років) з переліком іноземців чи осіб без громадянства (по одній чи декількох категоріях), що перетинали державний кордон України.

	Пункт пропуску	Дата перетину	Напрям	ПІБ (лат.)	Стать	Громадянство	Серія, № паспорта	Дата народження
2	Жуляни	03.11.2017 20:48	I	HENEED JEHEFEUR NOHENED SHEH NOW	F	Афганістан	U6761300	01.05.1975
3	Жуляни	03.11.2017 20:48	I	ELWIN LINS	F	Афганістан	M8121071	01.05.1975
4	Жуляни	03.11.2017 20:48	I	BEBU ERUN	F	Афганістан	R7865575	01.05.1975
5	Жуляни	03.11.2017 20:48	I	FUPTE ENERDEEP	F	Афганістан	U3149763	01.05.1975
6	Жуляни	03.11.2017 20:48	I	ENILCUNER EYSWERYE	F	Афганістан	N7600775	01.05.1975
7	Жуляни	03.11.2017 20:48	I	PEZHUNCELE SHEJI ENITTE	F	Афганістан	L6367137	01.05.1975
8	Жуляни	03.11.2017 20:48	I	CUNER DEB	F	Афганістан	M1963716	01.05.1975
9	Жуляни	03.11.2017 20:48	I	EJIL JOE EBREHEN	F	Афганістан	N1255120	01.05.1975
10	Жуляни	03.11.2017 20:48	I	JOSE EBIN	F	Афганістан	T4848419	01.05.1975
11	Жуляни	03.11.2017 20:48	I	SHEJI ETHUL	F	Афганістан	T1303190	01.05.1975
12	Жуляни	03.11.2017 20:48	I	VIDHYE LIBU	F	Афганістан	Z2892109	01.05.1975
13	Жуляни	03.11.2017 20:48	I	JOHNSON JYOTHIS	F	Афганістан	J5123745	01.05.1975
14	Жуляни	03.11.2017 20:48	I	LECSHNENEN ENUSHREE	F	Афганістан	N1568040	01.05.1975
15	Жуляни	03.11.2017 20:48	I	HOLCER SUJIT	F	Афганістан	S7326476	01.05.1975
16	Жуляни	03.11.2017 20:48	O	NURUFENENTHEN YEEFESH	F	Афганістан	M8861852	01.05.1975
17	Жуляни	03.11.2017 20:48	O	SWEPNE SUNIL SWETHI	M	Афганістан	R0840877	01.05.1975
18	Жуляни	03.11.2017 20:48	O	POOTHULLY JOHNY NEENE	F	Афганістан	V0131806	01.05.1975
19	Жуляни	03.11.2017 20:48	O	EBU SHIFES	M	Афганістан	N0582719	01.05.1975
20	Жуляни	03.11.2017 20:48	O	REJI RIJE NERIN	F	Афганістан	M0665282	01.05.1975
21	Жуляни	03.11.2017 20:48	O	THONES NERLIN	M	Афганістан	S5961404	01.05.1975
22	Жуляни	03.11.2017 20:48	O	PELEYIL VERIETH LECSHNIPRIYE	M	Афганістан	S1797242	01.05.1975
23	Жуляни	03.11.2017 20:48	I	EYSHETH NIHELE	F	Афганістан	Z2861725	01.05.1975
24	Жуляни	03.11.2017 20:48	O	VENCETESEN CISHORECUNER	M	Афганістан	R2117918	01.05.1975
25	Жуляни	03.11.2017 20:48	O	CEVUNCEL NEPPURETHU ENIL DEVU	F	Афганістан	T5827280	01.05.1975
26	Жуляни	03.11.2017 20:48	O	NEHES SHEENE ECTHER NOHENNED	M	Афганістан	R2117930	01.05.1975

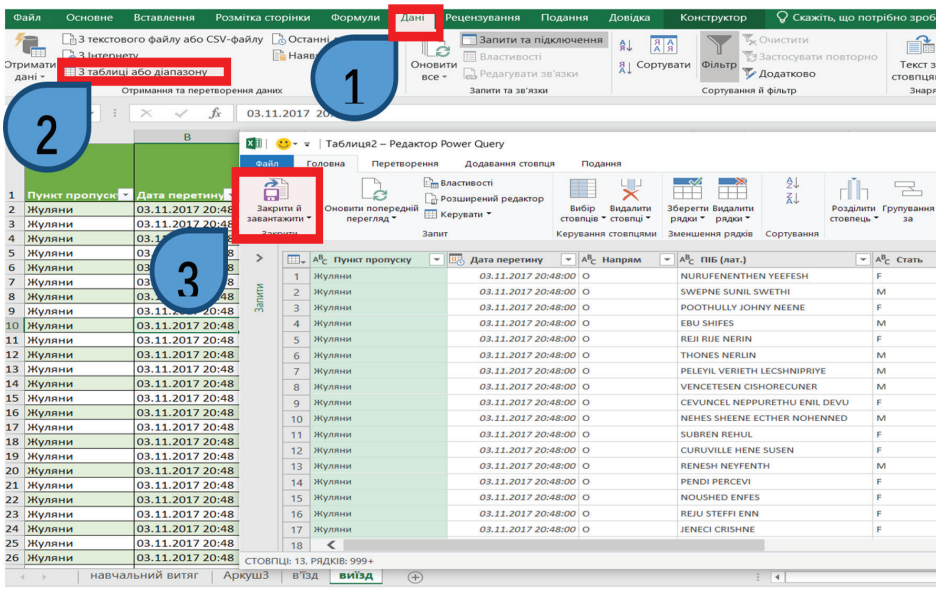
2. Розділити вищевказані дані на два окремих інформаційні масиви, із урахуванням напряму слідування.



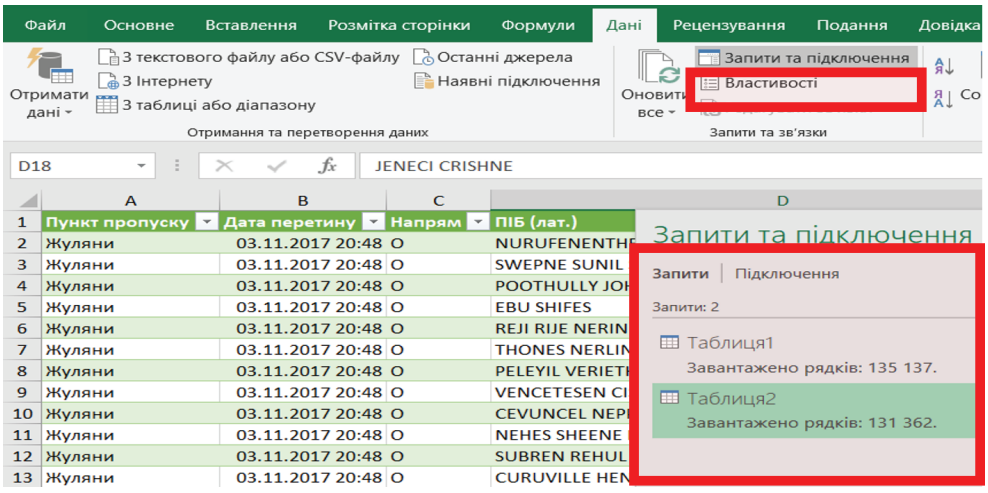
3. Виділити усю інформацію на кожному аркуші («в'їзд» і «виїзд») та встановити для них формат таблиці.



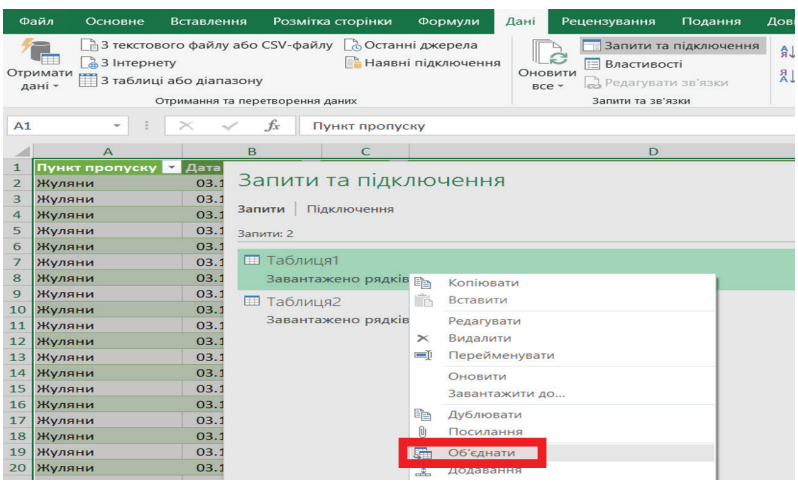
4. Створити запити з допомогою редактора Power Query (на основі інформації, що міститься на аркушах («в'їзд» і «виїзд»). Для цього на панелі вкладок перейти до розділу «Дані» і обрати кнопку «З таблиці або діапазону», після чого у вікні, що з'явиться натиснути кнопку «Закрити й завантажити».



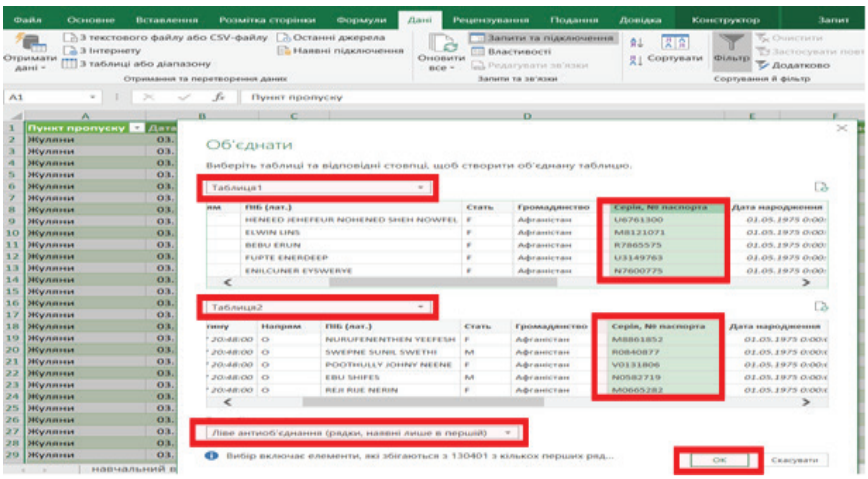
5. Після проведення вищевказаних дій в області завдань з'являться два запити, які містять інформацію з аркушів «в'їзд» і «виїзд».



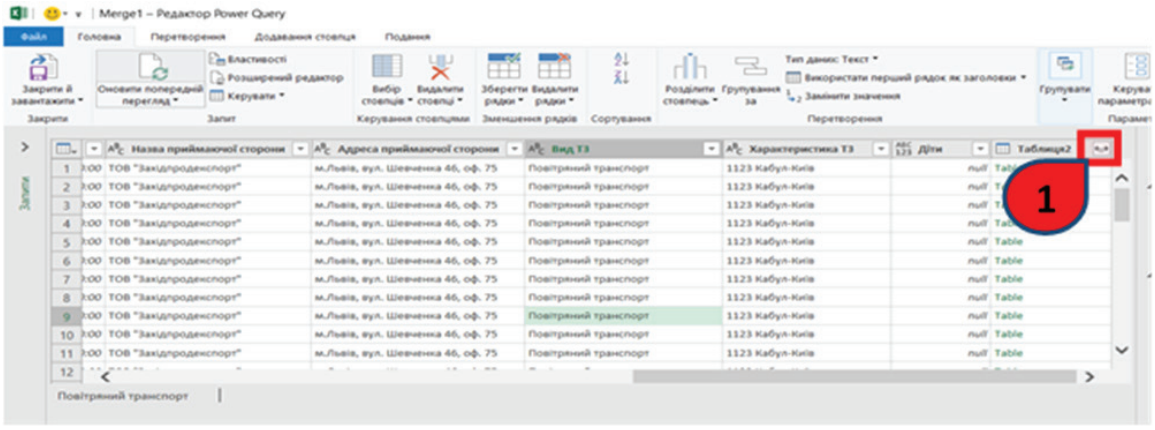
6. Об'єднати обидва сформовані запити. Для цього потрібно навести курсор миші на запит, що містить інформацію з аркуша «в'їзд» (в області завдань) і натиснути праву кнопку миші, а потім у контекстному меню вибрати команду «Об'єднати».

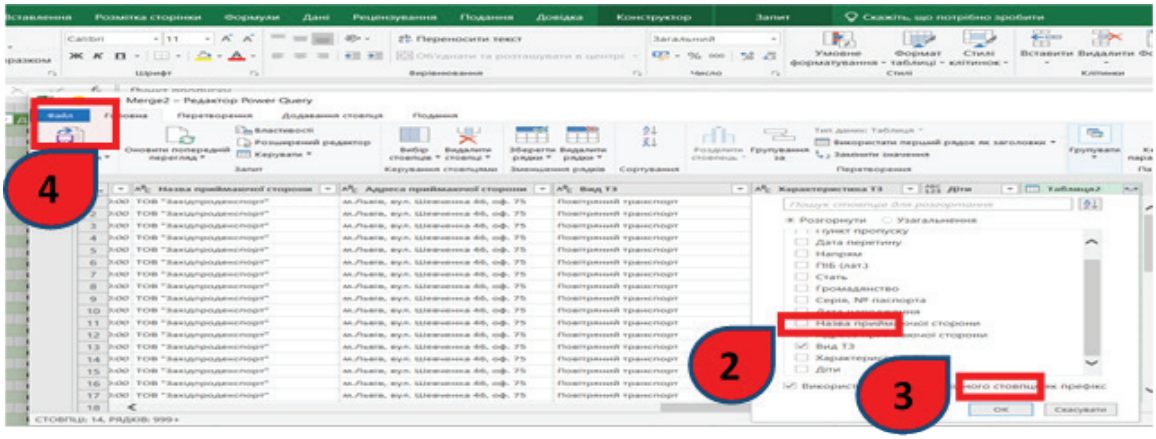


7. Встановити унікальні значення, що наявні у запиті сформованому із даних аркуша «в'їзд» та не повторюються у запиті сформованому із аркуша «виїзд». Для чого необхідно налаштувати поля вікна, що з'явиться наступним чином: вибрати таблиці, що потрібно об'єднати; встановити колонки, значення яких будуть порівнюватись при об'єднанні (серія, № паспорта або декілька інших колонок); задати параметр типу об'єднання «Ліве антиоб'єднання», рядки, наявні лише в першій.

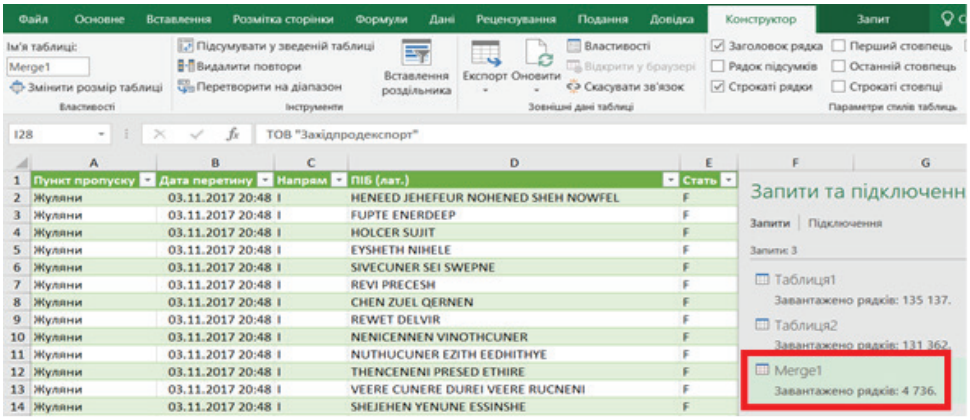


8. Після натискання кнопки «ОК» редактор Power Query сформує нову об'єднану таблицю, у відповідності до раніше здійснених налаштувань. При попередньому перегляді об'єднаної таблиці встановити, яка інформація нам потрібна з другого запиту і натиснути кнопку «Закрити й завантажити».

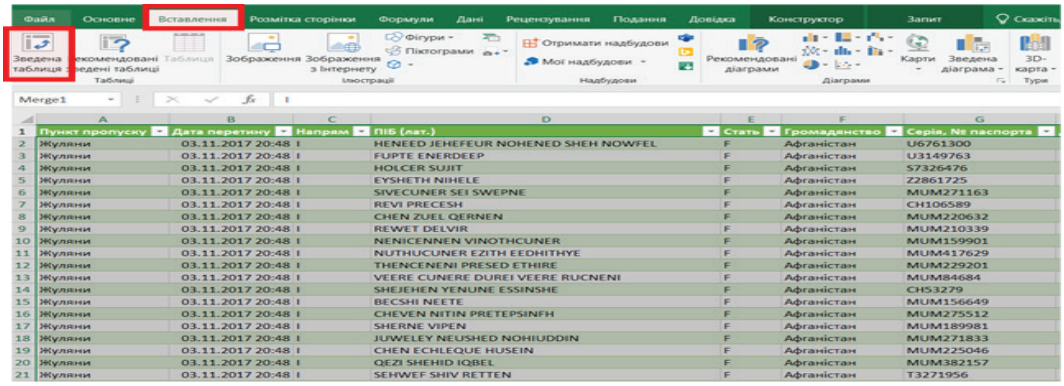




9. Після чого редактор Power Query сформує наступну таблицю.



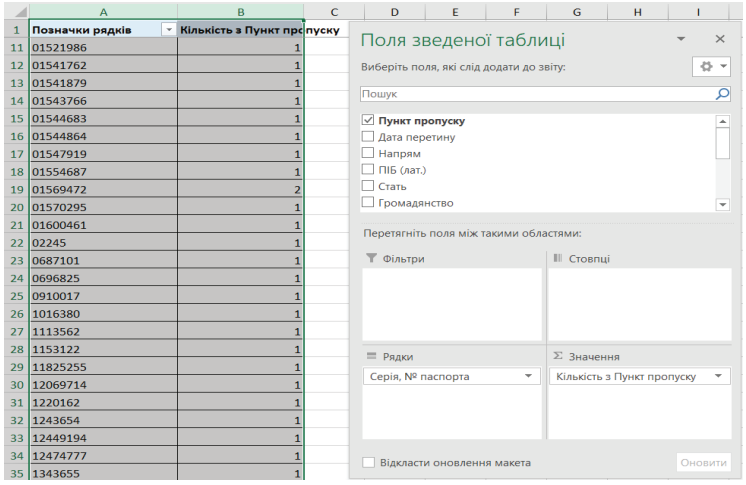
10.З використанням інформації із об'єднаної таблиці створити зведену таблицю, для встановлення наявності дублювання значень (ідентифікаторів, які порівнювались при формуванні об'єднаної таблиці). Наявність повторів відповідних значень вказує на можливі допущенні помилки персоналу ДПСУ при внесенні інформації щодо відповідної категорії осіб до ІТС «Гарт-1», або інші аспекти, які мають бути перевірені в окремому порядку. Так, необхідно виділити потрібний діапазон значень таблиці, на панелі вкладок перейти до розділу «Вставлення» і обрати кнопку «Зведена таблиця».



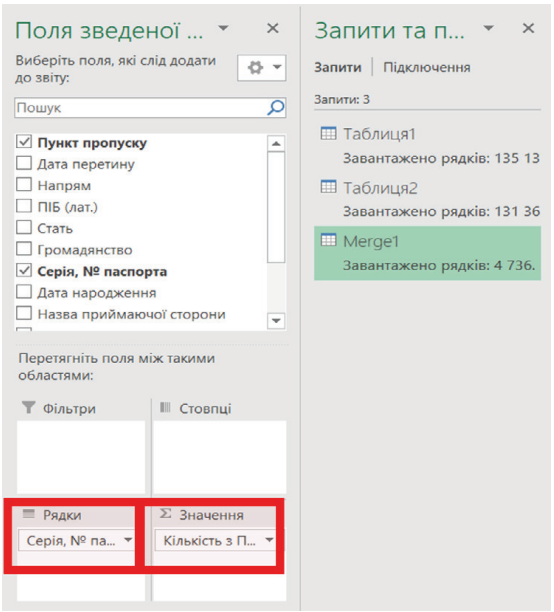
Пункт пропуску	Дата перетину	Напрям	ПІБ (лат.)	Стать	Громадянство	Серія, № паспорта
Жуляни	03.11.2017 20:48	I	HENEED JEHEFEUR NOHENED SHEH NOWFEL	F	Афганістан	U6761300
Жуляни	03.11.2017 20:48	I	FUPTE ENERDEEP	F	Афганістан	U3149763
Жуляни	03.11.2017 20:48	I	HOLCER SUHT	F	Афганістан	S7326476
Жуляни	03.11.2017 20:48	I	EYSHETH NIHELE	F	Афганістан	Z2861725
Жуляни	03.11.2017 20:48	I	SIVECUNER SEI SWEPNE	F	Афганістан	MUM271163
Жуляни	03.11.2017 20:48	I	REVI PRECESH	F	Афганістан	CH106589
Жуляни	03.11.2017 20:48	I	CHEN ZUEL QERNEN	F	Афганістан	MUM220632
Жуляни	03.11.2017 20:48	I	REWET DELVIR	F	Афганістан	MUM210339
Жуляни	03.11.2017 20:48	I	NENICENNEN VINOTHCUNER	F	Афганістан	MUM159901
Жуляни	03.11.2017 20:48	I	NUTHUCUNER EZITH EEDHITHYE	F	Афганістан	MUM417629
Жуляни	03.11.2017 20:48	I	THENCENENI PRESED ETHIRE	F	Афганістан	MUM229201
Жуляни	03.11.2017 20:48	I	VEERE CUNERE DUREI VEERE RUCNENI	F	Афганістан	MUM84684
Жуляни	03.11.2017 20:48	I	SHEJEHEN YENUNE ESSINSHE	F	Афганістан	CH53279
Жуляни	03.11.2017 20:48	I	BECSHI NEETE	F	Афганістан	MUM156649
Жуляни	03.11.2017 20:48	I	CHEVEN NITIN PRETEPSINFH	F	Афганістан	MUM275512
Жуляни	03.11.2017 20:48	I	SHERNE VIPEN	F	Афганістан	MUM189981
Жуляни	03.11.2017 20:48	I	JUWELEY NEUSHED NOHIUDDIN	F	Афганістан	MUM271833
Жуляни	03.11.2017 20:48	I	CHEN ECHLEQUE HUSEIN	F	Афганістан	MUM225046
Жуляни	03.11.2017 20:48	I	QEZI SHEHID IQBEL	F	Афганістан	MUM382157
Жуляни	03.11.2017 20:48	I	SEHWEF SHIV RETTEN	F	Афганістан	T3271956

11. Налаштування параметрів вікна, що з'явиться («Створення зведеної таблиці») залишити без змін і натиснути кнопку «ОК».

12. Налаштувати поля зведеної таблиці, шляхом перетягування потрібних назв колонок до областей «Рядки» та «Значення».

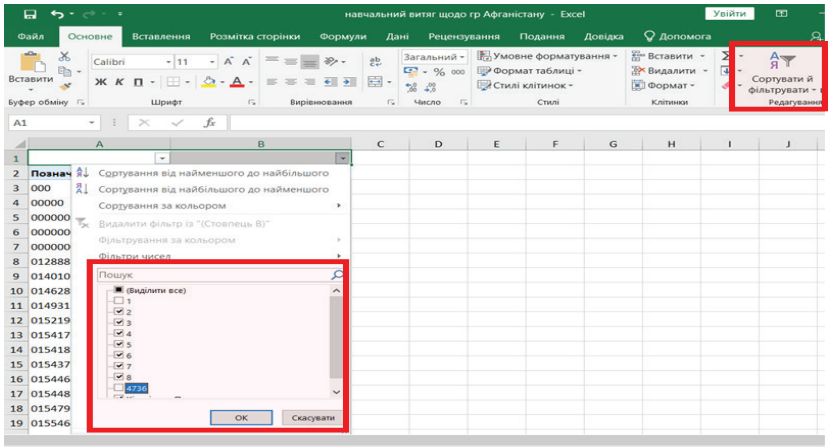


Позначки рядків	Кількість з Пункт пропуску
01521986	1
01541762	1
01541879	1
01543766	1
01544683	1
01544864	1
01547919	1
01554687	1
01569472	2
01570295	1
01600461	1
02245	1
0687101	1
0696825	1
0910017	1
1016380	1
1113562	1
1153122	1
11825255	1
12069714	1
1220162	1
1243654	1
12449194	1
12474777	1
1343655	1



13. У результаті отримаємо наступну зведену таблицю.

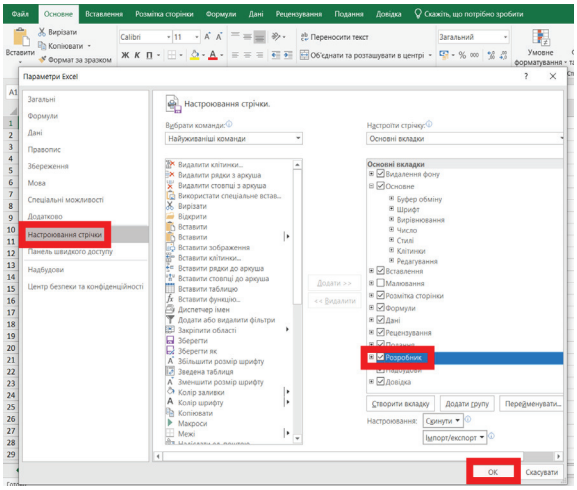
14. Для відокремлення паспортних документів, які повторюються у списку в декількох випадках, потрібно скористатись кнопкою «Фільтр» (розділу «Основне» на панелі вкладок) і здійснити фільтрування даних (виділити усі паспортні документи, що повторюються 2 рази або більше)



15.Здійснити додаткову перевірку сформованих списків у підсистемах ІТС «Гарт-1». Відпрацювати звіт щодо результатів проведених заходів.

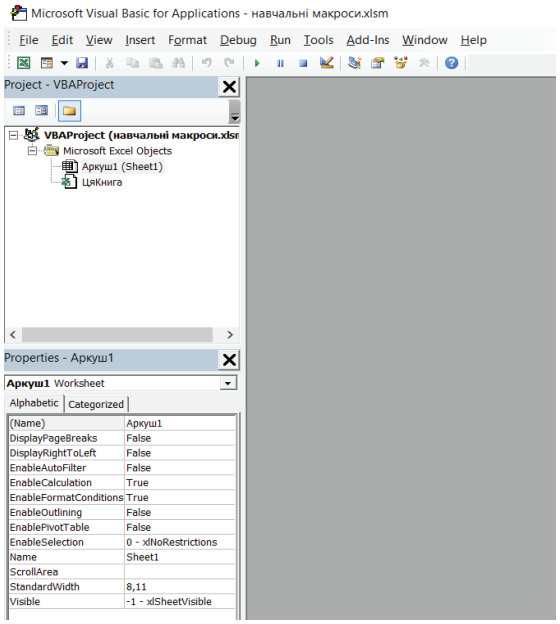
Автоматизація завдань, що системно повторюються, опрацювання та редагування великих масивів даних налаштування взаємодії Microsoft Excel з іншими програмами з використанням макросів та засобів Visual Basic Application (VBA).

Якщо при роботі з Microsoft Excel виникла необхідність кілька разів виконати одну і ту ж послідовність дій, то можна записати відповідну послідовність як макрос. Макрос – це дія або набір дій, які можна виконати скільки завгодно раз.



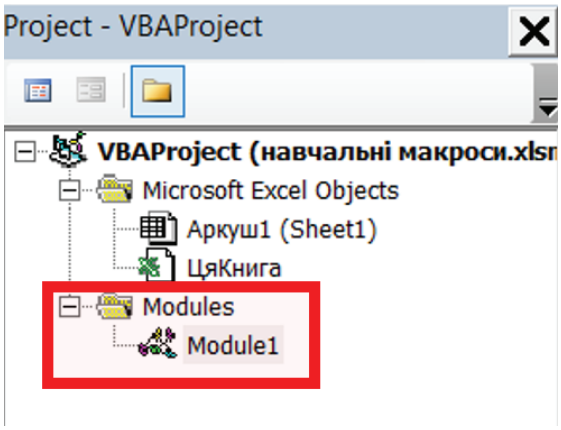
1. Макрос записується на мові Visual Basic for Applications. Створений макрос можна викликати для виконання з основного меню за допомогою кнопки на панелі інструментів або на робочій області, а також комбінації клавіш (Alt+F8). Макроси і засоби VBA можна знайти на вкладці «Розробник», яка по замовчуванню є прихована.

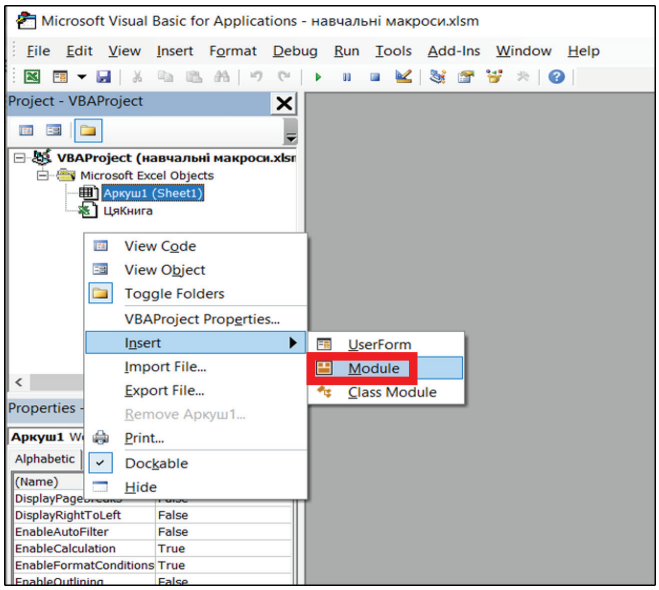
Для того, щоб додати до стрічки вкладку «Розробник» необхідно на панелі вкладок перейти до розділу «Файл» і натиснути кнопки «Параметри» → «Настроювання стрічки», у списку «Основні вкладки» встановити галочку біля пункту «Розробник» і натиснути кнопку «ОК».



Способи формування макросів: написання макросів «з нуля»; використання готових макросів; редагування макросів знайдених у мережі Інтернет; макрорекодер (інструмент для запису дій користувача і перетворення їх у програмний код).

2. Для створення і редагування макросів необхідно зберігати файл в форматі «.xlsm» (книга Excel із підтримкою макросів). При створенні макросу використовується редактор Visual Basic Editor. Для швидкого відкриття даного редактора потрібно скористатись комбінацією клавіш «Alt + F11», після чого буде відображено нижчевказане вікно.

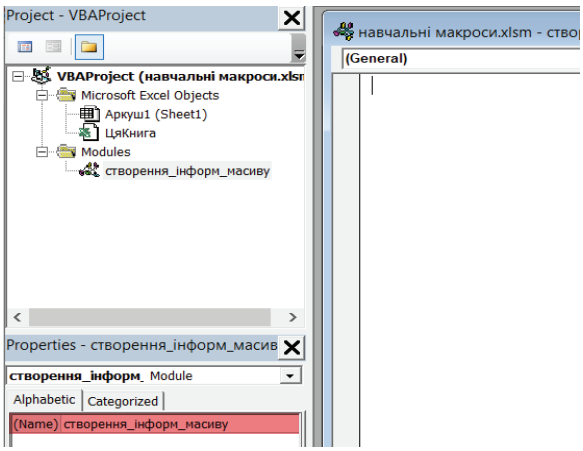




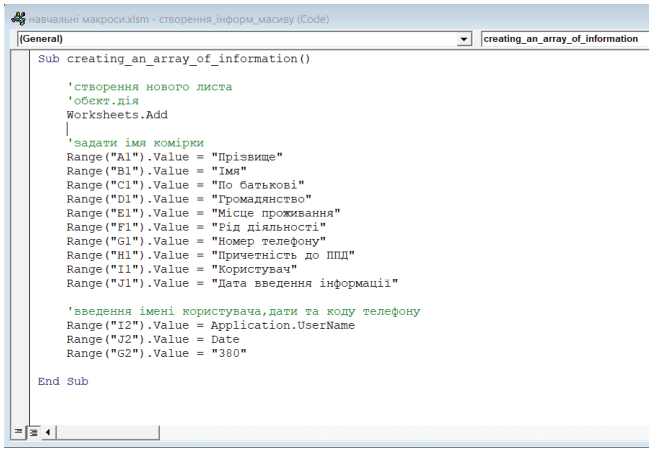
3. Перед початком написання макросу необхідно створити модуль, в якому зберігатиметься програмний код макросу. Для цього у вікні «Project» потрібно натиснути ПКМ, обрати пункт «Insert» → «Module».

4. Після чого у вікні «Project» з'явиться папка «Modules» і файл «Module1».

5. У подальшому доцільно перейменувати створений модуль. Для чого необхідно у вікні «Project» виділити створений модуль, а у вікні «Properties» змінити його назву (пробіли у назві не допускаються).



6. Створюємо код макросу. Для зразку розглянемо варіант написання простого макросу, який в книзі Excel створить новий аркуш і сформує на ньому таблицю (інформаційний масив) із частковим автоматичним заповненням окремих її колонок. Приклад написання вищевказаного макросу наведено нижче.




```
Sub creating_an_array_of_information()

    'створення нового листа
    'обєкт.дія
    Worksheets.Add

    'задати імя комірки
    Range("A1").Value = "Прізвище"
    Range("B1").Value = "Імя"
    Range("C1").Value = "По батькові"
    Range("D1").Value = "Громадянство"
    Range("E1").Value = "Місце проживання"
    Range("F1").Value = "Рід діяльності"
    Range("G1").Value = "Номер телефону"
    Range("H1").Value = "Причетність до ППД"
    Range("I1").Value = "Користувач"
    Range("J1").Value = "Дата введення інформації"

    'введення імені користувача,дати та коду телефону
    Range("I2").Value = Application.UserName
    Range("J2").Value = Date
    Range("G2").Value = "380"

End Sub
```

Так, для кожного макросу обов'язкова наявність операторів **Sub** і **End Sub**.

Creating_an_array_of_information – ім'я макросу (бажано писати латинськими літерами).

' – символ коментаря. Рядок макросу, який розпочинається з даного символу носить виключно довідковий характер для автора макросу та осіб, які в майбутньому будуть його використовувати.

Worksheets.Add – добавити новий аркуш до книги Excel.

Range("A1").Value = "Прізвище" – звернення до конкретної комірки таблиці, для вставлення туди текстового значення (Прізвище).

Value – ім'я процедури, що здійснює доступ до властивостей конкретної комірки.

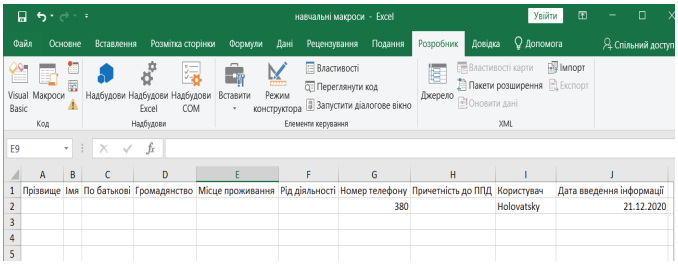
Range("I2").Value = Application.UserName – звернення до конкретної комірки таблиці, для вставлення туди імені користувача.

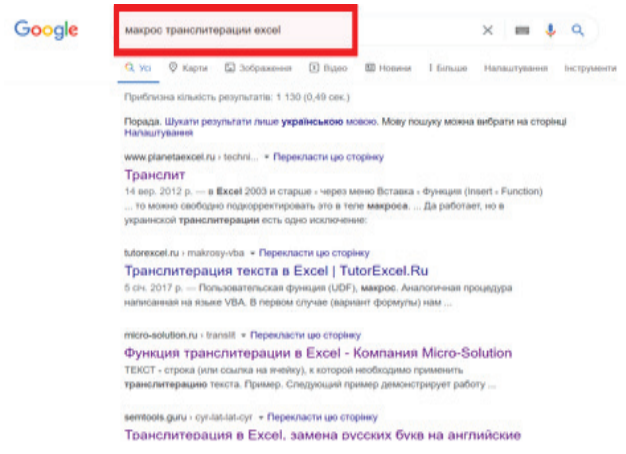
Range("J2").Value = Date – звернення до конкретної комірки таблиці, для вставлення туди дати.

7. Для застосування макросу потрібно натиснути кнопку «Run/Sub» (клавіша F5), для перевірки правильності написання окремих частин макросу необхідно скористатись режимом покрокового запуску макросу (клавіша F8). Розміщення кнопки «Run/Sub» наведено нижче.

8. За умов правильного написання відповідного макросу в книзі Excel буде створено нижче вказаний аркуш.

9. Даний макрос необхідно вставляти в кожну окрему книгу, в якій його потрібно використовувати.





Якщо є необхідність створення певного макросу, то з метою економії робочого часу, для його написання, доцільно здійснити пошук відповідного макросу в мережі Інтернет. Так, для прикладу розглянемо варіант коли у аналітика є необхідність здійснити транслітерацію прізвищ та імен великої кількості громадян Російської Федерації (з російської на англійську).

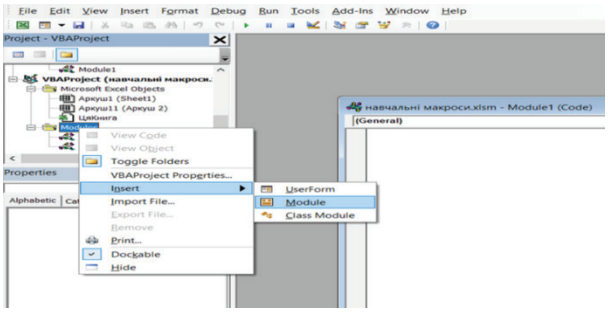
Для пошуку вищевказаного макросу скористаємось пошуковим сервісом Google.

В ході вивчення результатів пошуку (аналіз коментарів до відповідних статей) потрібно вибрати макрос, який іншим користувачам вдалось успішно застосувати для вирішення їхніх питань.

В подальшому в книзі Excel потрібно відкрити редактор Visual Basic (Alt+F11) і у вікні «Project» потрібно натиснути ПКМ та обрати пункт «Insert» → «Module».



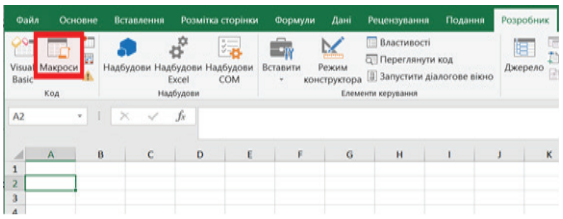
Вставляємо скопійований код макросу у вікно редактора коду і приводимо його у відповідність до законодавчих норм країни, громадяни якої вказані у вихідних даних (у нашому випадку Російська Федерація).

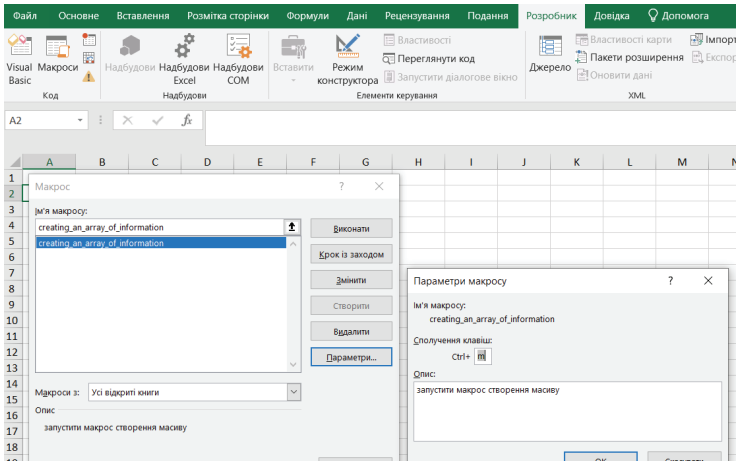




За результатами редагування вихідного коду для приведення його функціоналу до законодавчих норм рф, отримаємо наступний код макросу.

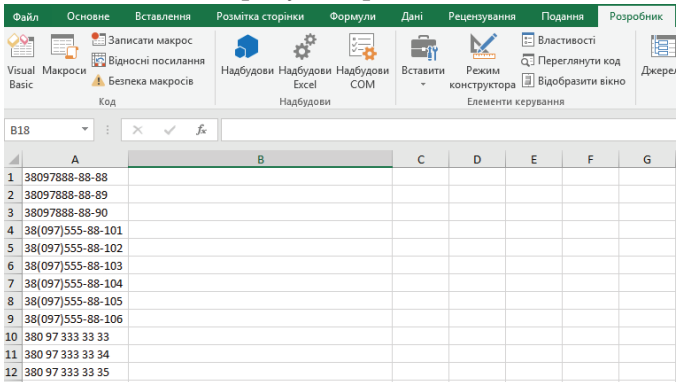
Для швидкого запуску макросу на будь-якому аркуші книги можна налаштувати здійснення даної дії із використанням комбінації клавіш. Для цього потрібно перейти на вкладку «Розробник», в групі «Код» натиснути кнопку «Макроси».





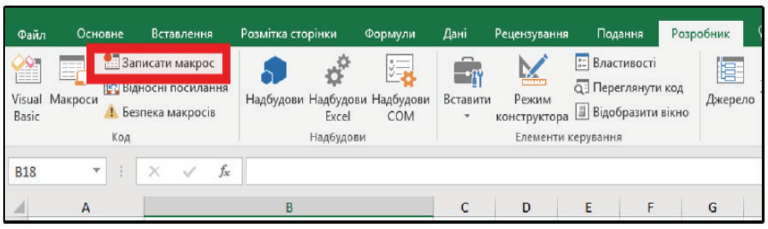
У полі «Ім'я макросу», вибрати макрос для якого потрібно призначити комбінацію клавіш і натиснути кнопку «Параметри», у полі «Сполучення клавіш» ввести бажану комбінацію та заповнити поле «Опис», натиснути кнопку «ОК».

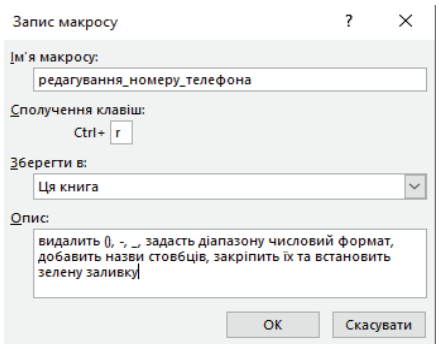
Також для створення макросу можна використовувати макрорекодер. Макрорекодер – це інструмент в Excel, який покроково записує усі дії користувача в даній програмі і перетворює їх в код на мові VBA. Код макросу створеного з допомогою макрорекодера в подальшому можна відредагувати.



Для прикладу створення макросу з використанням макрорекодера розглянемо варіант опрацювання масиву телефонних номерів (із різними форматами відображення даних). Так, змоделюємо варіант, коли аналітику надали масив даних з телефонними номерами, які потрібно привести до єдиного зразку і перевірити з використанням наявних можливостей (відкриті джерела, бази даних державних установ).

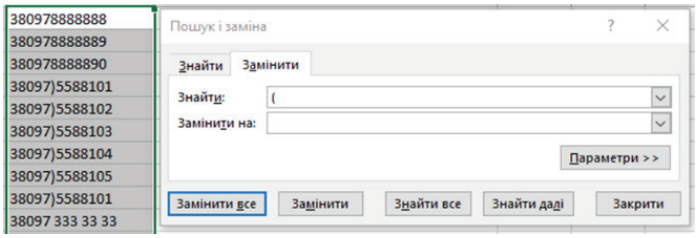
Для збереження усіх проведених дії і перетворення їх на код макросу потрібно натиснути кнопку «Записати макрос» (на вкладці «Розробник»)



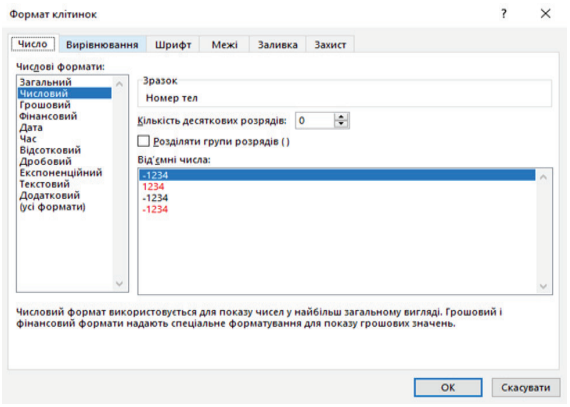


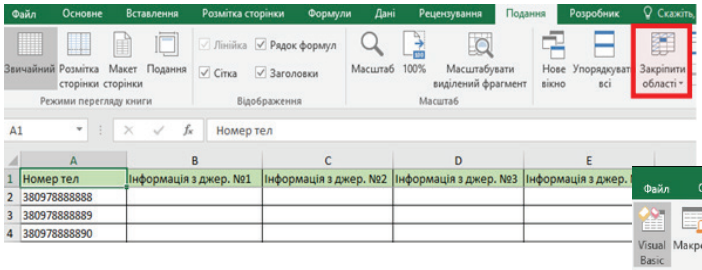
Після застосування вищевказаної команди з'явиться вікно, в якому необхідно буде визначити ім'я макросу, сполучення «гарячих клавіш», місце збереження макросу та опис дій, які здійснюватиме макрос і натиснути кнопку «ОК».

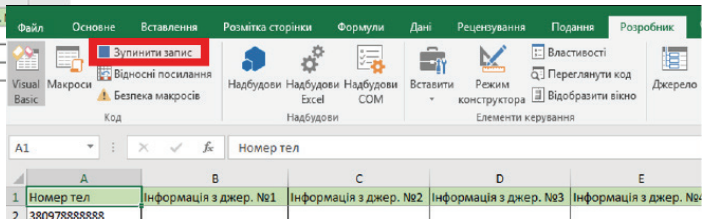
Згодом, усі дії, що виконуватимуться в програмі Excel будуть записуватись та переводитись у код макросу, а саме:



- Виділення стовчика та видалення із нього непотрібних символів («CTRL+H» натиснути кнопку «Замінити все»);
- Задаємо числовий формат клітинок, де містяться телефонні номери;
- Добавляємо назви стовпчиків і виділяємо їх кольором;
- Закріплюємо назви стовпчиків;





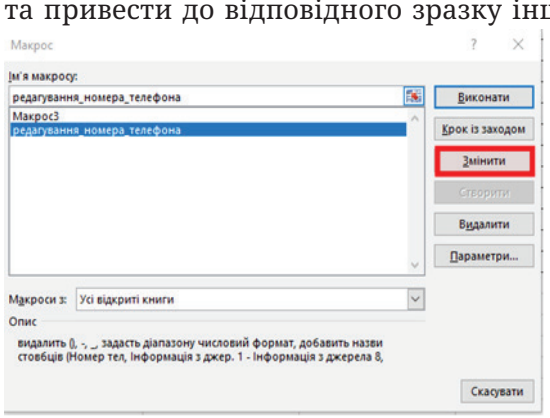


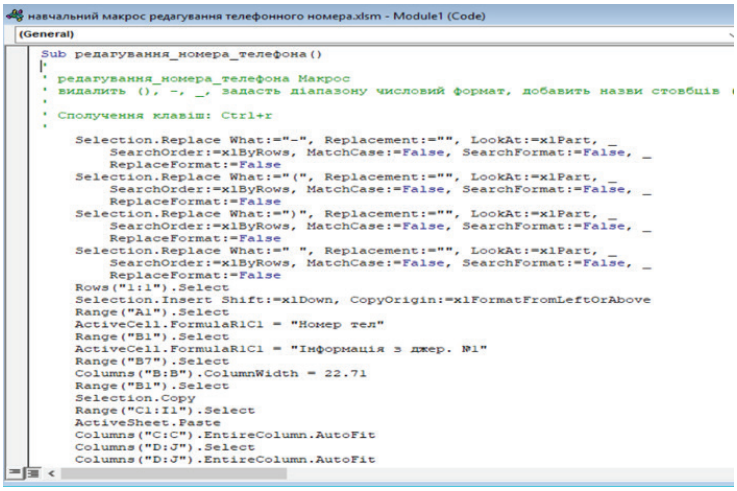
- Натискаємо кнопку «Зупинити запис».

Для перегляду чи редагування створеного коду макросу потрібно перейти на вкладку «Розробник» натиснути кнопку «Макроси», обрати відповідний макрос та натиснути кнопку «Змінити».

Після чого відкриється редактор Visual Basic, у вікні редактора коду можна переглянути чи редагувати код макросу, який ми створили з допомогою макрорекодера;

Якщо в подальшому виникатиме необхідність повторити вищевказаний перелік дій та привести до відповідного зразку інші

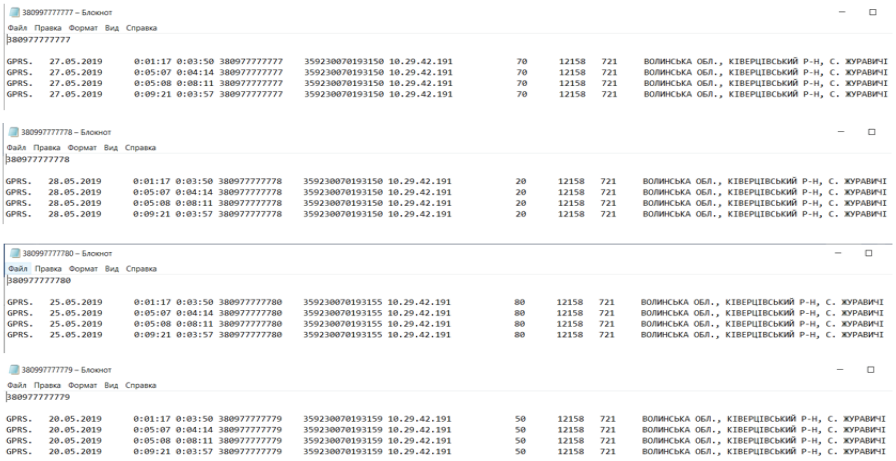




списки з телефонними номерами то достатньо буде натиснути комбінацію клавіш «Ctrl+r» і макрос, який ми створили із використанням макрорекодера здійснить їх автоматично.

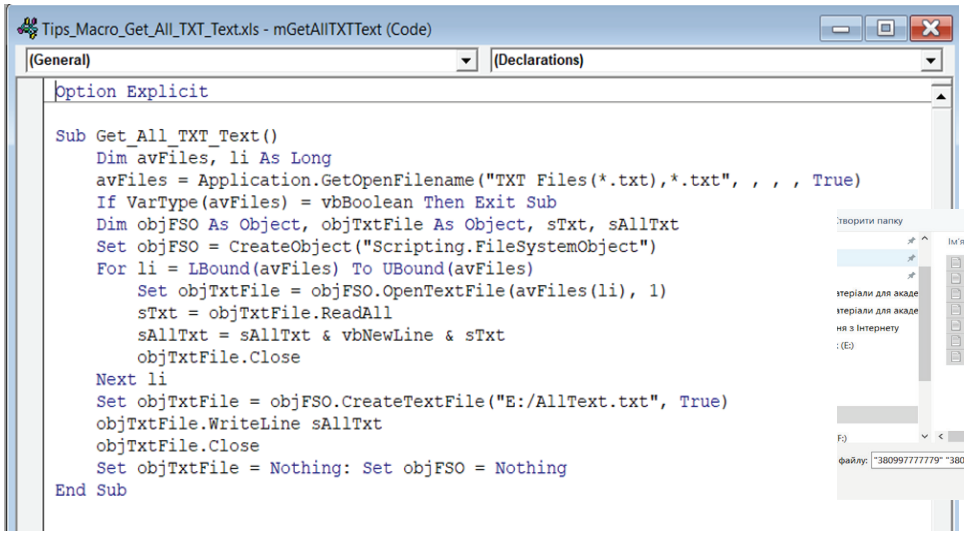
Слід зазначити, що макроси можуть виконувати операції з файлами за межами поточного документа. Так, макроси можуть використовуватись для: пошуку визначеної інформації у вказаному каталозі чи переліку певних файлів; відправки даних Excel в документ у форматі Word; відправки даних Excel в презентації PowerPoint; запуску макросу Access з Excel; створення, видалення або редагування файлів; об'єднання декількох документів в один файл; автоматизації виконання багатьох інших завдань.

Для прикладу використання макросів при роботі з файлами за межами поточного документа розглянемо ситуацію коли кримінальному аналітику необхідно об'єднати інформацію з семи файлів текстового формату в один.

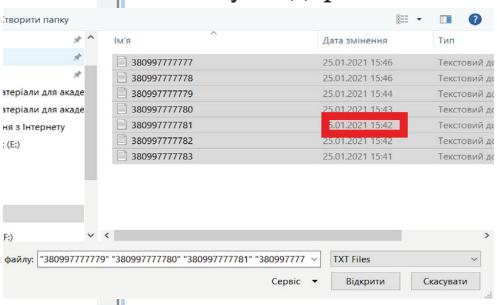


Кожен із перелічених файлів містить інформацію, яка стосується відповідного телефонного номера. Вміст даних файлів наведено нижче:

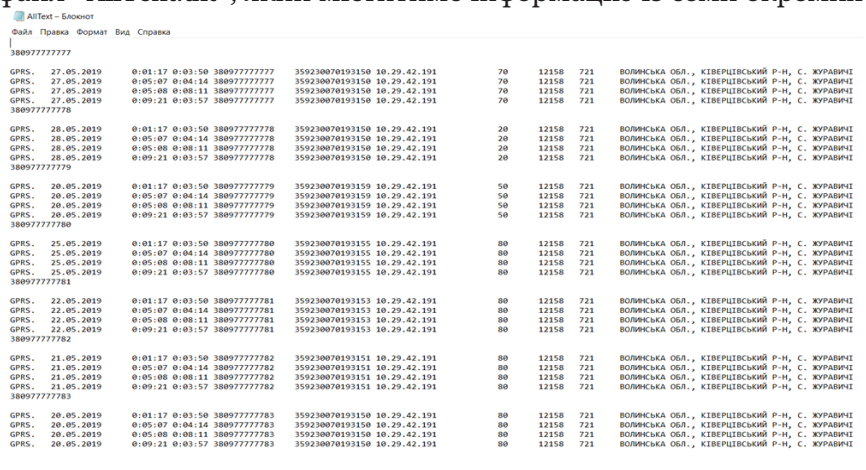
Для об'єднання інформації з вищевказаних файлів в один файл будемо використовувати наступний макрос.



Характерною особливістю даного макросу є те, що після його запуску потрібно виділити усі файли, які необхідно об'єднати в один файл та натиснути кнопку «Відкрити».



Після чого на диску «E» з'явиться файл «AllText.txt», який міститиме інформацію із семи окремих текстових файлів.



Завдяки широким можливостям мови і зручній моделі поширення (з файлами документів) макроси Microsoft Office довгий час використовуються для створення та розповсюдження шкідливого програмного забезпечення - макровірусів. Незважаючи на посилення налаштувань, пов'язаних з макросами (на поточний момент актуальні версії Microsoft Office при налаштуваннях по замовчанню забороняють автоматичне виконання макросів, повідомляючи про це користувача), макровіруси активно застосовуються зловмисниками і зараз. З цієї причини запускайте і дозволяйте виконання макросів тільки з джерел, яким Ви довіряєте або здійснюйте ці дії з використанням додаткових заходів захисту, таких, як середовище віртуальної машини.

Інформаційно-технологічний прогрес вимагає від співробітників різних установ та органів постійного вдосконалення професійних навичок, які дозволяють ефективно виконувати посадові обов'язки. Для отримання нових знань та умінь уже давно не обов'язково вступати на навчання у ВНЗ чи проходити окремі курси. Так, в мережі Інтернет наявна дуже велика кількість навчальних матеріалів (відеоматеріали, конспекти, публікації, презентації, інформація з форумів та інше) з різних галузей діяльності.

АНАЛІЗ ТЕЛЕФОННИХ З'ЄДНАНЬ

Аналіз білінгів проводиться, відповідно до заданої мети, використовуючи програмне забезпечення **Microsoft Excel** та **i2 Analyst`s Notebook**, тому приклади будуть розглядатися у декількох варіантах.

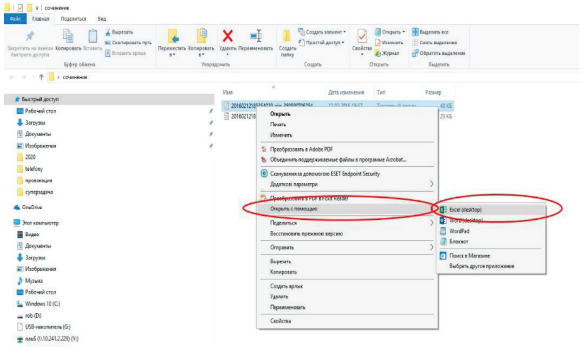
Отримання телефонних білінгів (*деталізація фактів телефонних з'єднань, можливо назва «роздруківка», іноді називають «трафік»*) здійснюється виключно в рамках ухвали суду і отримується у відповідних центрах оперативно-технічних заходів правоохоронних структур та безпосередньо їх можна отримати у оператора стільникового зв'язку. Для спрощення в подальшому будемо називати це – білінг.

У рамках кримінального аналізу білінгу можна встановити активність фігурантів, використання декількох номерів чи мобільних терміналів, зв'язки з власниками інших телефонних номерів, частоту та тривалість розмов, місцезнаходження та маршрути слідування, перебування в одній місцевості з іншими абонентами та інші завдання.

Кожен окремий аналіз має свою мету та завдання, тому шляхи до їх вирішення мають дещо відмінний і специфічний характер. У будь-якому випадку дослідження телефонних з'єднань побудовано на виявленні закономірностей чи, навпаки, відмінностей від щоденного ритму життя абонента.

Різновиди білінгів, з якими працюють аналітики. Білінги бувають декількох типів:

Білінг ТАТВ – в одному файлі зафіксовані дані абонента ТА – це основний номер телефону відносно якого здійснюється дослідження, ТВ – це номери телефонів контактів абонента ТА.



Файл, у переважній більшості приходить у форматі **.txt**, для відкриття його використовуємо *Microsoft Excel:*

При отриманні білінгів файл складається з трьох частин:

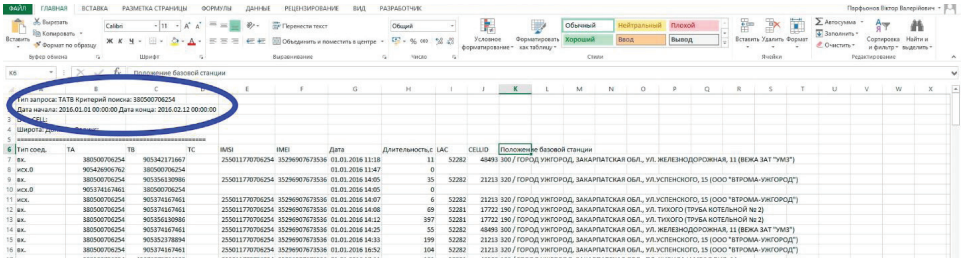
перша частина – інформаційна, знаходиться у верхній частині файлу;

друга частина – основна таблиця білінгу;

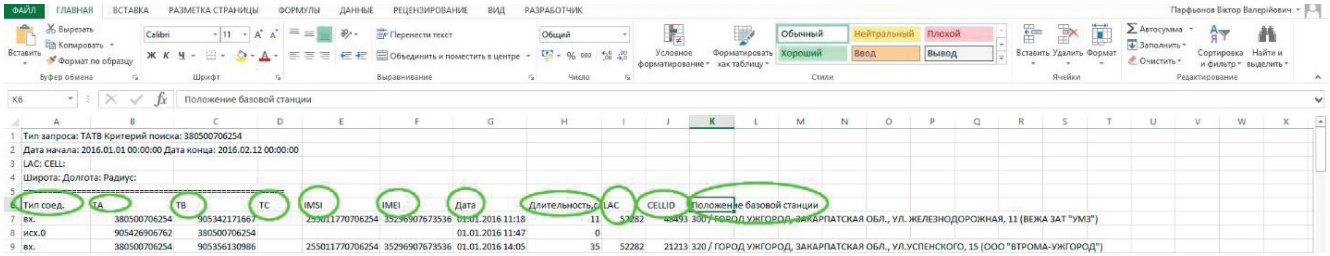
третя частина – статистка білінгу.

У першій частині вказано номер телефону відносно якого був створений білінг, дата початку та завершення білінгу.

Білінг може бути по номеру телефона, тоді у верхній стрічці буде зазначений номер телефону, або білінг може бути по терміналу (IMEI), тоді у верхній стрічці буде вказано номер IMEI.



У деяких випадках білінг ТАТВ буває в двох файлах, один це ТА, другий – ТВ, для цього необхідно

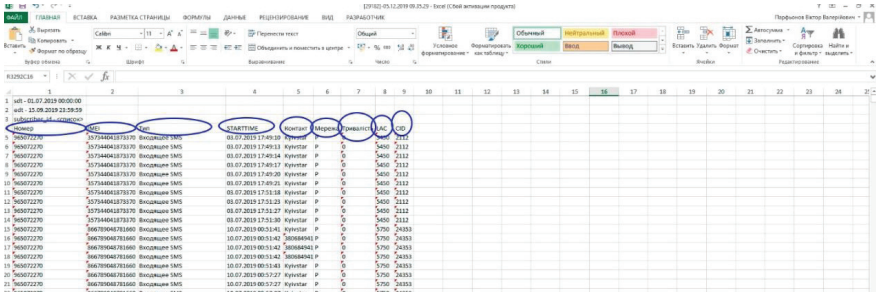


засобами Microsoft Excel з'єднати другі частини файлів в єдину таблицю, тоді файл перетвориться до формату білінгу ТАТВ.

У білінгах є наступні стовпці (зазначаються мовою оригіналу):
«Тип з'єднання» - вид та напрям з'єднання (вхідний чи вихідний дзвінок, вхідне чи вихідне смс-повідомлення, інтернет-з'єднання (GPRS), переадресація).

«ТА» - номер телефону, який здійснює або отримує з'єднання (*відповідно до напряму з'єднання з п.1*).
«ТВ» - номер телефону (*сервісна послуга*) іншого абонента, який з'єднувався з абонентом з п. 2.
«ТС» - номер телефону, з якого здійснювалась переадресація.
«IMSI» - унікальний номер сім-картки абонента з п. 2.
«IMEI» - унікальний номер стільникового терміналу абонента з п. 2.
«Дата» - Дата та час з'єднання.
«Тривалість, с» - Тривалість з'єднання (розмови, інтернет-трафіку).
«LAC» – код місцевості (Location Area Code) мереж GSM, в якій розташована базова станція стільникового зв'язку абонента з п. 2.
«CELLID» – ідентифікатор соти (Cell ID) базової станції стільникового зв'язку абонента з п. 2.

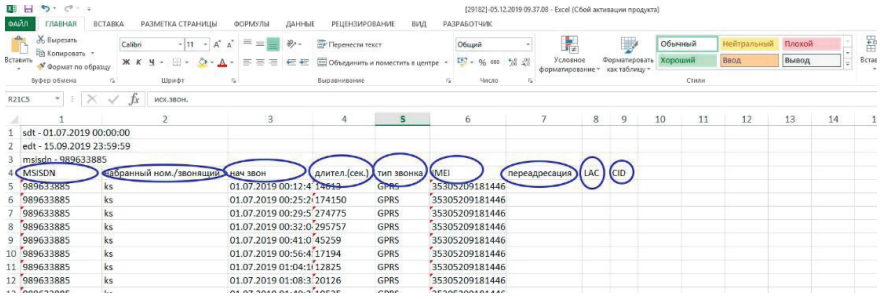
«Положення базової станції» - азимут місця знаходження терміналу абонента з п. 2 та базова станція стільникового зв'язку, в якій він перебував.



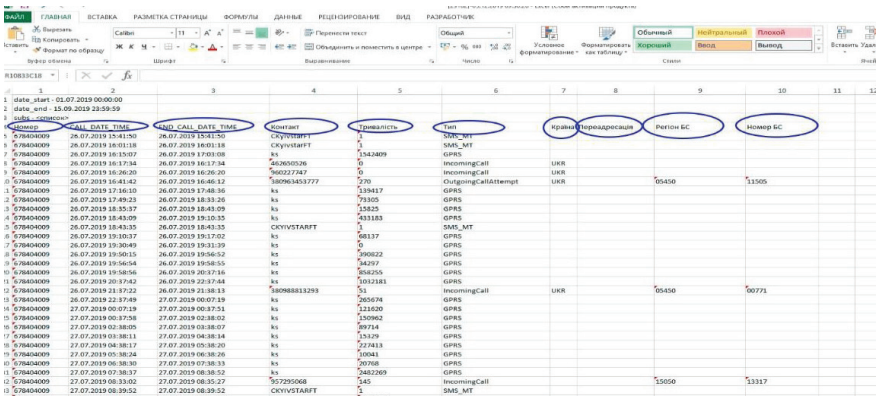
Білінг ТА – принципово не відрізняється від білінгу ТАТВ, одна відмінність, що в колонці **ТА** буде лише один номер телефона, який вказано в першій частині файлу.

Білінг IMEI – принципово не відрізняється від білінгу ТАТВ, одна відмінність, що в колонці **ТА** будуть лише номер (номери) телефону, SIM-карти, яких вставлялись до мобільного терміналу на IMEI якого було отримані білінги та який вказано в першій частині файлу.

Білінг оператора – як правило, складається з декількох файлів, три з них, файли самого білінгу та один файл розшифровки місця знаходження веж стільникового зв'язку.

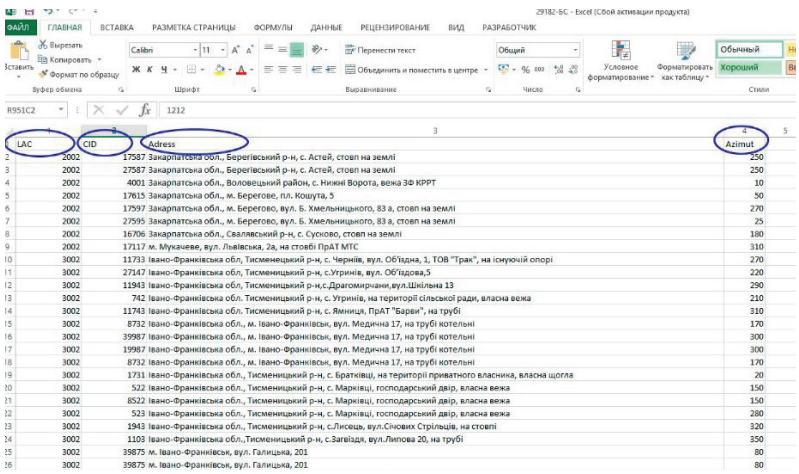


MSISDN	Набранный ном./звонящий	нач звон	длител.(сек.)	тип звонка	IMEI	переадресация	LAC	CID
989633885	ks	01.07.2019 00:12:4	14613	GPRS	353052091814 46			
989633885	ks	01.07.2019 00:25:2	174150	GPRS	353052091814 46			
989633885	ks	01.07.2019 00:29:5	274775	GPRS	353052091814 46			
989633885	ks	01.07.2019 00:32:0	295757	GPRS	353052091814 46			
989633885	ks	01.07.2019 00:41:0	45259	GPRS	353052091814 46			
989633885	ks	01.07.2019 00:56:4	17194	GPRS	353052091814 46			
989633885	ks	01.07.2019 01:04:1	12825	GPRS	353052091814 46			
989633885	ks	01.07.2019 01:08:3	20126	GPRS	353052091814 46			



date_start - 01.07.2019 00:00:00								
date_end - 15.09.2019 23:59:59								
subs_common								
Номер	CALL_DATE_TIME	END_CALL_DATE_TIME	Контакт	Тривалість	Тип	Країна	Переадресація	Регіон БС	Номер БС
678404009	26.07.2019 15:41:50	26.07.2019 15:41:50	CKYIVSTARFT	1	SMS_MT				
678404009	26.07.2019 16:01:18	26.07.2019 16:01:18	CKyivstarFT	1	SMS_MT				
678404009	26.07.2019 16:15:07	26.07.2019 17:03:08	ks	1542409	GPRS				
678404009	26.07.2019 16:17:34	26.07.2019 16:17:34	462650526	0	IncomingCall	UKR			
678404009	26.07.2019 16:26:20	26.07.2019 16:26:20	960227247	0	IncomingCall	UKR			
678404009	26.07.2019 16:41:42	26.07.2019 16:46:12	380963453777	270	OutgoingCallAttempt	UKR		05450	11505
678404009	26.07.2019 17:16:10	26.07.2019 17:48:36	ks	139417	GPRS				
678404009	26.07.2019 17:49:23	26.07.2019 18:33:26	ks	79305	GPRS				
678404009	26.07.2019 18:35:37	26.07.2019 18:43:09	ks	15825	GPRS				
678404009	26.07.2019 18:43:09	26.07.2019 19:10:35	ks	43183	GPRS				
678404009	26.07.2019 18:43:35	26.07.2019 18:43:35	CKYIVSTARFT	1	SMS_MT				
678404009	26.07.2019 19:10:37	26.07.2019 19:17:02	ks	68137	GPRS				
678404009	26.07.2019 19:30:49	26.07.2019 19:31:19	ks	0	GPRS				
678404009	26.07.2019 19:50:15	26.07.2019 19:56:52	ks	390822	GPRS				
678404009	26.07.2019 19:56:54	26.07.2019 19:58:55	ks	34297	GPRS				
678404009	26.07.2019 19:59:06	26.07.2019 20:37:16	ks	858255	GPRS				
678404009	26.07.2019 20:37:42	26.07.2019 22:37:44	ks	1012181	GPRS				
678404009	26.07.2019 21:37:22	26.07.2019 21:38:13	380988813293	51	IncomingCall	UKR		05450	00771
678404009	27.07.2019 22:37:49	27.07.2019 00:07:19	ks	265674	GPRS				
678404009	27.07.2019 00:07:19	27.07.2019 00:37:51	ks	121620	GPRS				
678404009	27.07.2019 00:37:58	27.07.2019 02:38:02	ks	150962	GPRS				
678404009	27.07.2019 02:38:05	27.07.2019 03:38:07	ks	89714	GPRS				
678404009	27.07.2019 03:38:11	27.07.2019 04:38:14	ks	15329	GPRS				
678404009	27.07.2019 04:38:17	27.07.2019 05:38:20	ks	227413	GPRS				
678404009	27.07.2019 05:38:24	27.07.2019 06:38:26	ks	10041	GPRS				
678404009	27.07.2019 06:38:30	27.07.2019 07:38:33	ks	20768	GPRS				
678404009	27.07.2019 07:38:37	27.07.2019 08:38:52	ks	248269	GPRS				
678404009	27.07.2019 08:33:02	27.07.2019 08:35:27	957295068	145	IncomingCall			15050	13317
678404009	27.07.2019 08:39:52	27.07.2019 08:39:52	CKYIVSTARFT	1	SMS_MT				

Основною відмінністю цих білінгів є те, що положення базової станції знаходиться в окремому файлі. Перед проведенням аналізу, рекомендовано привести такий білінг до вигляду «**білінгу ТАТВ»**. Поля «**білінгу ТАТВ**», які описані вище, співпадають із полями, які знаходяться е трьох файлах цього білінгу, окрім поля «Положення базової станції», це поле формується шляхом співставлення параметрів «LAC» та «SID» файлу білінгу з даних із файлу в якому вказані адреси базових станцій. Цей процес можна здійснювати вручну, шляхом сортування стовпчиків «LAC» та «SID» і потім здійснення співставлення, або в автоматичному режимі із використанням функції **Microsoft Excel**, яка називається «**ВПР»** (в англійській версії VLOOKUP), як користуватися можливостями цієї функції можна знайти в посібнику користувача **Microsoft Excel.**

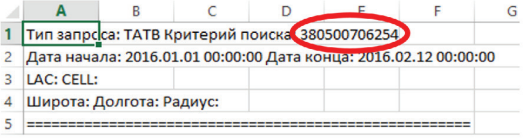


LAC	CID	Adress	Azimut
2002	17587	Закарпатська обл., Берегівський р-н, с. Астей, стовп на землі	250
2002	27587	Закарпатська обл., Берегівський р-н, с. Астей, стовп на землі	250
2002	4001	Закарпатська обл., Воловецький район, с. Нижні Ворота, вежа ЗФ КРРТ	10
2002	17615	Закарпатська обл., м. Берегове, пл. Кошута, 5	50
2002	17597	Закарпатська обл., м. Берегово, вул. Б. Хмельницького, 83 а, стовп на землі	270
2002	27595	Закарпатська обл., м. Берегово, вул. Б. Хмельницького, 83 а, стовп на землі	25
2002	16706	Закарпатська обл., Свалявський р-н, с. Сусково, стовп на землі	180
2002	17117	м. Мукачеве, вул. Львівська, 2а, на стовбі ПрАТ МТС	310
3002	11733	Івано-Франківська обл, Тисменецький р-н, с. Чернів, вул. Об'їздна, 1, ТОВ "Трак", на існуючій опорі	270
3002	27147	Івано-Франківська обл, Тисменицький р-н, с.Угринів, вул. Об'їздова,5	220
3002	11943	Івано-Франківська обл. Тисменицький р-н,с.Драгомирчани,вул.Шкільна 13	290
3002	742	Івано-Франківська обл. Тисменицький р-н, с. Угринів, на території сільської ради, власна вежа	210
3002	11743	Івано-Франківська обл. Тисменицький р-н, с. Ямниця, ПрАТ "Барви", на трубі	310
3002	8732	Івано-Франківська обл., м. Івано-Франківськ, вул. Медична 17, на трубі котельні	170
3002	39987	Івано-Франківська обл., м. Івано-Франківськ, вул. Медична 17, на трубі котельні	300
3002	19987	Івано-Франківська обл., м. Івано-Франківськ, вул. Медична 17, на трубі котельні	300
3002	8732	Івано-Франківська обл., м. Івано-Франківськ, вул. Медична 17, на трубі котельні	170
3002	1731	Івано-Франківська обл., Тисменицький р-н, с. Братківці, на території приватного власника, власна щогла	20
3002	522	Івано-Франківська обл., Тисменицький р-н, с. Марківці, господарський двір, власна вежа	150
3002	8522	Івано-Франківська обл., Тисменицький р-н, с. Марківці, господарський двір, власна вежа	150
3002	523	Івано-Франківська обл., Тисменицький р-н, с. Марківці, господарський двір, власна вежа	280
3002	1943	Івано-Франківська обл., Тисменицький р-н, с.Лисець, вул.Січових Стрільців, на стовпі	320
3002	1103	Івано-Франківська обл.,Тисменицький р-н, с.Завівдя, вул.Липова 20, на трубі	350
3002	39875	м. Івано-Франківськ, вул. Галицька, 201	80
3002	39875	м. Івано-Франківськ, вул. Галицька, 201	80

Отже, рекомендовано приводити будь-який білінг до єдиного взірця, що в подальшому надає можливість зручніше проводити його аналіз. Описані нижче алгоритми та методики описані для вже приведених білінгів до формату «**білінг ТАТВ»**.

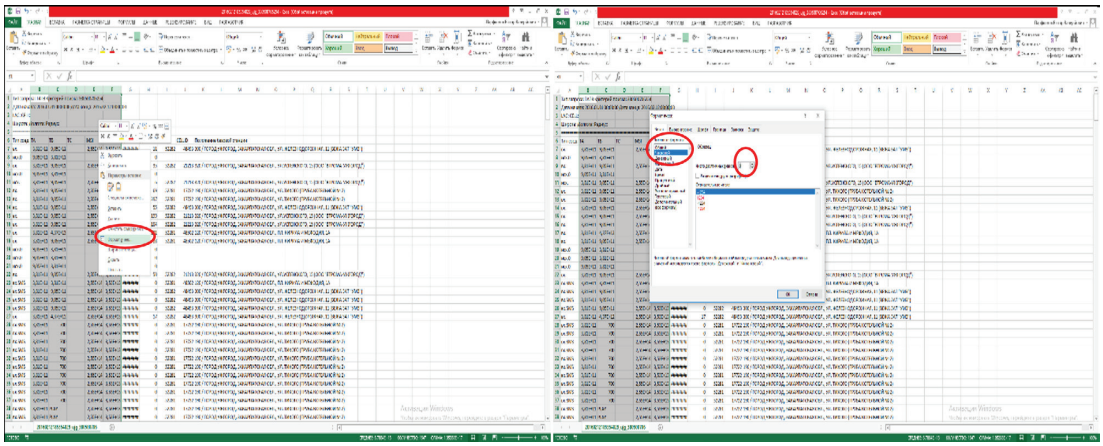
Алгоритм переведення білінгу до Microsoft Excel. У першу чергу, з білінгу встановлюється номер досліджуваного телефону, це видно, як правило, в заголовку файлу білінгу та в першій стрічці цього файлу.

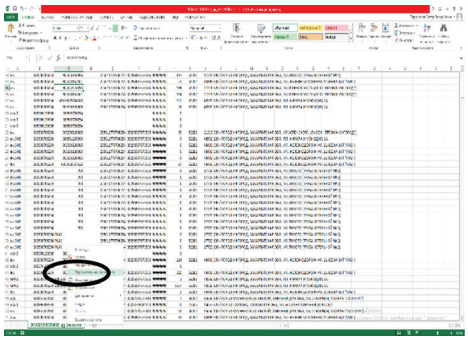


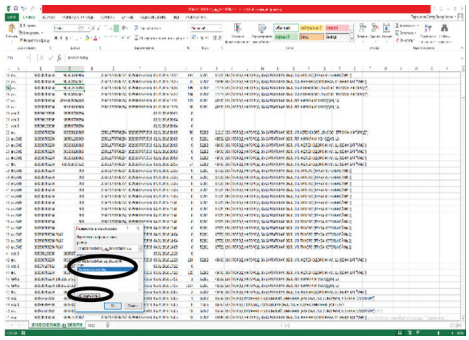


Для зручності переведемо білінг до Microsoft Excel, приблизно наступним алгоритмом:

Відкриваємо файл білінгу приводимо поля **TA, TB, TC, IMSI, IMEI** до числового формату, шляхом виділення відповідних стовпчиків у прикладі це стовпчики **B, C, D, E, F** натискаючи праву кнопку миші (або CTRL+1) вибираємо опцію **«Формат вічка…»**, вкладку **«Число»**, числовий формат **«Числовий»**, число десяткових знаків **«0».**







Робимо копію листа в **Microsoft Excel** шляхом натискання правої кнопки миші на назві листа, вибираємо «Скопіювати /Перемістити» переміщуємо в «перемістити в кінець», встановити маркер «створити копію», потім отриманий лист перейменовуємо, в нашому випадку було перейменовано на «*copy*» та переходим на неї.

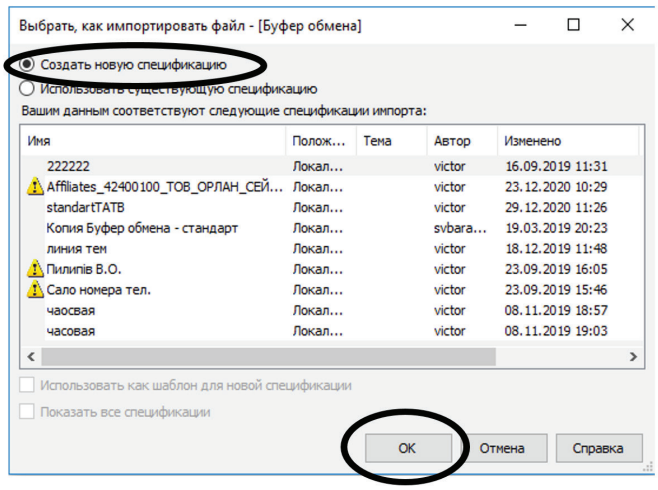
Приводимо до зручного вигляду, видаляємо перші строки, строки, які йдуть наприкінці після строки «=====СТАТИСТИКА=====» (*якщо така є*). Виставляємо фільтри першої стрічки: курсор на полі «Тип з'єднання», натискаємо гарячі клавіши **«CTRL+SHIFT+L»**, для зручності можна зробити межі клітинок (*операція не обов'язкова*), таблиця має приблизно такий вигляд:

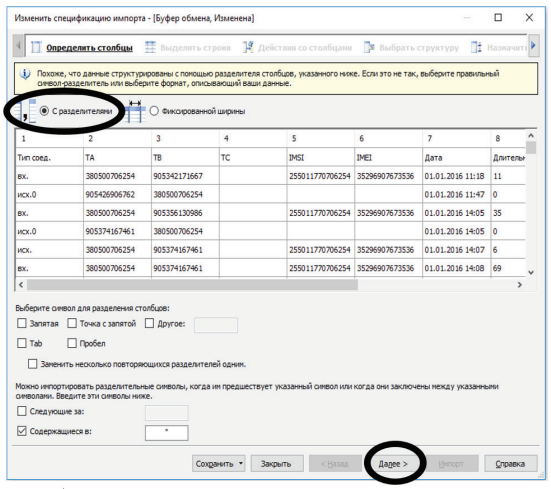
A	B	C	D	E	F	G	H	I	J	K
Тип сое	TA	TB	TC	IMSI	IMEI	Дата	Длительность	LAC	CELLID	Положение базовой станции
вх.	380500706254	905342171667		255011770706254	352969076735361	01.01.2016 11:18	11	52282	48493	300 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ЖЕЛЕЗНОДОРОЖНАЯ, 11 (ВЕЖА ЗАТ "УМЗ")
исх.0	905426906762	380500706254				01.01.2016 11:47	0			
вх.	380500706254	905356130986		255011770706254	352969076735361	01.01.2016 14:05	35	52282	21213	320 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ.УСПЕНСКОГО, 15 (ООО "ВТРОМА-УЖГОРОД")
исх.0	905374167461	380500706254				01.01.2016 14:05	0			
исх.	380500706254	905374167461		255011770706254	352969076735361	01.01.2016 14:07	6	52282	21213	320 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ.УСПЕНСКОГО, 15 (ООО "ВТРОМА-УЖГОРОД")
вх.	380500706254	905374167461		255011770706254	352969076735361	01.01.2016 14:08	69	52281	17722	190 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ТИХОГО (ТРУБА КОТЕЛЬНОЙ № 2)
вх.	380500706254	905356130986		255011770706254	352969076735361	01.01.2016 14:12	397	52281	17722	190 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ТИХОГО (ТРУБА КОТЕЛЬНОЙ № 2)
вх.	380500706254	905374167461		255011770706254	352969076735361	01.01.2016 14:25	55	52282	48493	300 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ЖЕЛЕЗНОДОРОЖНАЯ, 11 (ВЕЖА ЗАТ "УМЗ")
вх.	380500706254	905352378894		255011770706254	352969076735361	01.01.2016 14:33	199	52282	21213	320 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ.УСПЕНСКОГО, 15 (ООО "ВТРОМА-УЖГОРОД")
вх.	380500706254	905374167461		255011770706254	352969076735361	01.01.2016 16:52	104	52282	21213	320 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ.УСПЕНСКОГО, 15 (ООО "ВТРОМА-УЖГОРОД")
вх.	380500706254	43676879764388		255011770706254	352969076735361	01.01.2016 17:11	121	52281	48502	120 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., ПЛ. КИРИЛА И МЕФОДИЯ, 1А
вх.	380500706254	905356130986		255011770706254	352969076735361	01.01.2016 17:26	28	52281	48502	120 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., ПЛ. КИРИЛА И МЕФОДИЯ, 1А
исх.0	905356130986	380500706254				02.01.2016 20:03	0			

Алгоритм переведення білінгу до i2 Analyst`s Notebook:

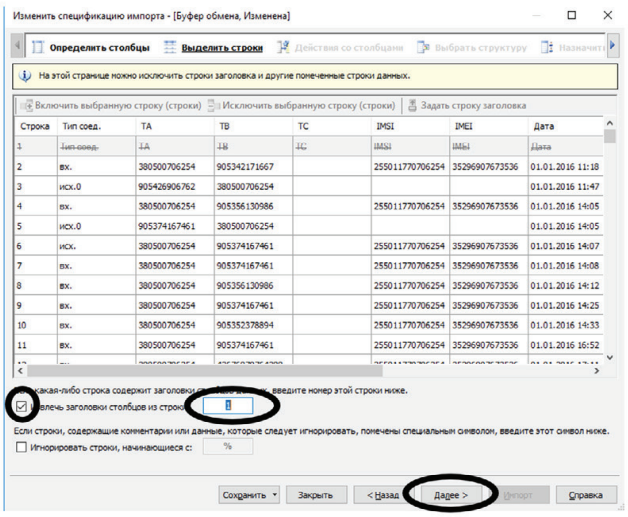
1. На підготовленому листі виділяємо всю таблицю: курсор на комірці **«A1»**, натискаємо **«CTRL+SHIFT+END»**, копіюємо в буфер обміну **«CTRL+C».**
2. Відкриваємо **I2 Analyst`s Notebook** вибираємо в меню **«Імпорт»**, **«Імпорт із буфера обміну…».**
3. У вікні натискаємо **«Продовжити».**
4. Вибираємо **«Створити нову специфікацію»** та натискаємо **«ОК»**.

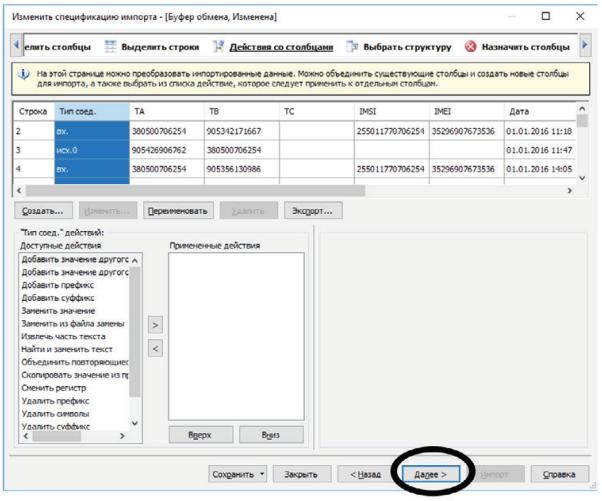
5. Запускається майстер створення специфікацій крок 1 – перевіряємо основні налаштування і натискаємо **«Далі»**.
6. Визначаємо заголовок та натискаємо **«Далі»**.



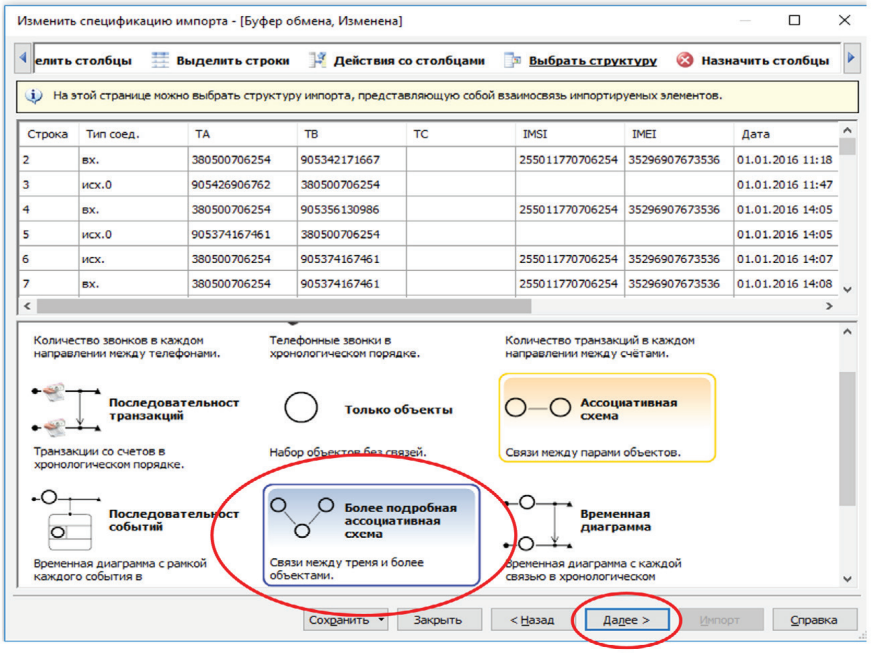


7. Якщо немає необхідності доставляти якихось суфіксів та префіксів, то наступний крок натискаємо кнопку **«Далі»**.





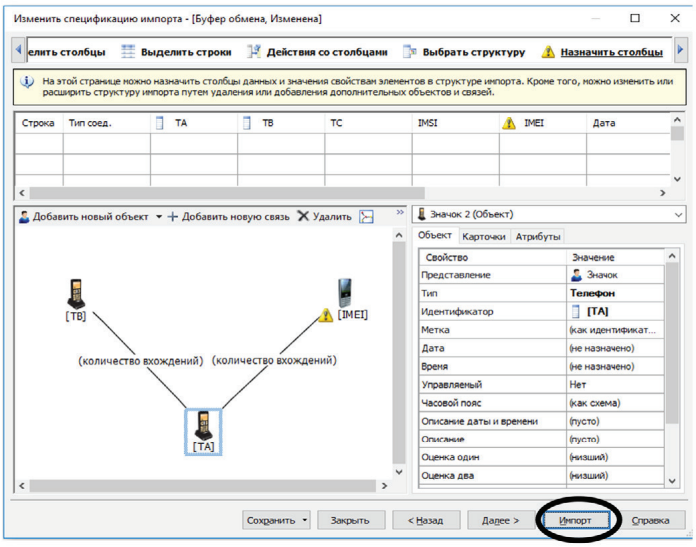
8. Наступним кроком обираємо варіант **«Більш детальна асоціативна схема»** натискаємо **«Далі»**.
9. Отримаємо вікно формування схеми, в якій шляхом перетаскування відповідного стовпчика формується сама схема. На зв'язках встановлюємо: «множинність з'єднання» - «одинарний», мітка - «кількість входжень». На об'єктах: там де абоненти ТА або ТВ встановлюємо тип – «Телефон», IMEI тип – «Мобільний телефон». Можна ще додавати до зв'язків карточки в яких буде зберігатися інша інформація з білінгу, проте ця операція на бажання самого аналітика.



На виході має бути вигляд приблизно, як відображено на малюку.

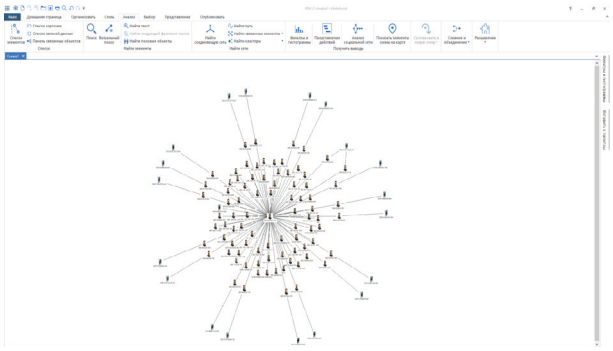
У разі наявності пустих полів в якомусь з полів, які є задіяні в схемі на розсуд аналітика, буде задано питання щодо пропуску внесення цих даних, чи внесення порожніх даних під час формування схеми.

Коли готова схема натискаємо **«ІМПОРТ»**.



Програма здійснить запит на збереження цієї специфікації. Рекомендовано зберегти, тому як, у майбутньому ті всі кроки не потрібно буде робити, а відразу відкрити відносно стандарту та зручну схему простого **білінгу ТАТВ**.

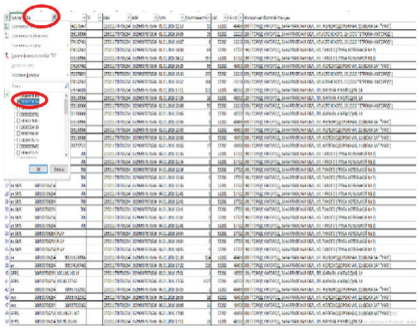
Після формування на робочому полі **I2 Analyst`s Notebook** з'явиться робоча схема з якою в подальшому здійснюються аналітичні маніпуляції.

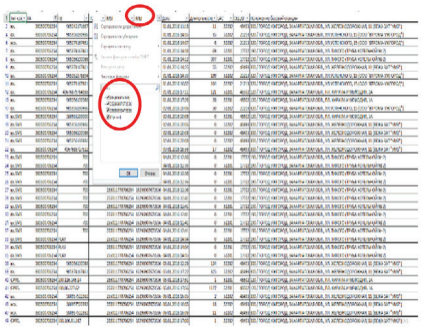


У подальшому аналіз буде здійснюватися за допомогою самого білінга в **Microsoft Excel** та схеми в **I2 Analyst`s Notebook.**

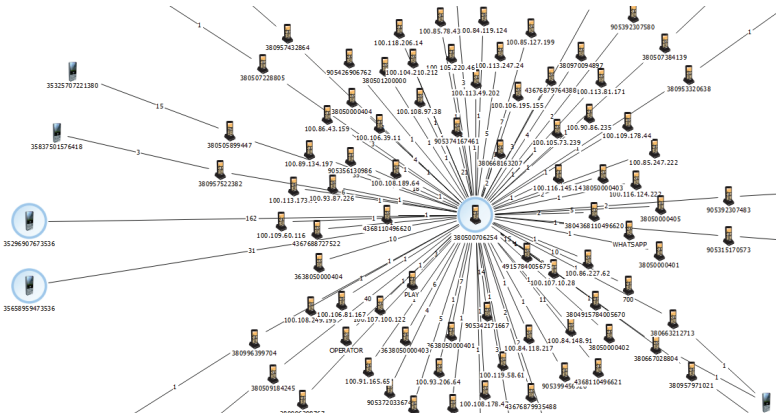
Алгоритм визначення кількості терміналів. Для визначення мобільних терміналів, у яких використовувався номер телефону, можна використати **Microsoft Excel, а саме:**

1. Встановлюємо фільтр на стрічці заголовку.
2. У стовпчику ТА вибираємо лише досліджуваний телефон і ставим по ньому фільтр.
3. У графі IMEI залишаться IMEI і через фільтр цього стовпчика можна буде побачити їх кількість та по даті можна визначити в який день (дні) в якому з терміналів використовувалась картка.





На схемі одразу видно скільки і які номери терміналів використовував абонент.

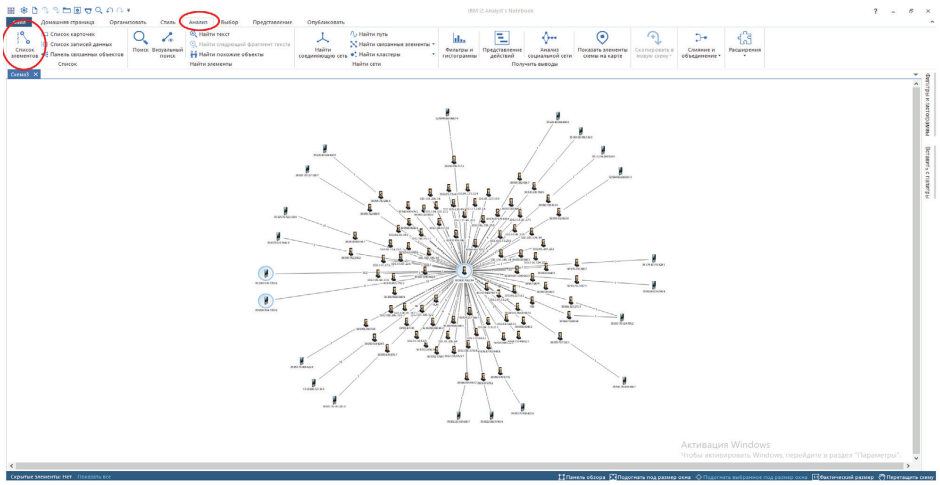


4. Таким чином, нам вдалось встановити чи користувався абонент декількома терміналами. Подальшим аналізом можна здійснити пошук, по наявним масивам даних чи хтось ще колись користувався цими терміналами.

При аналізі білінга, який був отриманий на термінал – алгоритм подібний, єдине що необхідно врахувати, що в цьому білінгу буде відображено в графі **ТА** всі номери стільникового зв'язку, які перебували в терміналі, а по датах можна встановити коли відбувались заміни та де перебував абонент. Для більш зручної роботи із схемою та подальшим аналізом необхідно забрати GPRS з'єднання, «іменовані» з'єднання (SMS з'єднання із різноманітними сервісами).

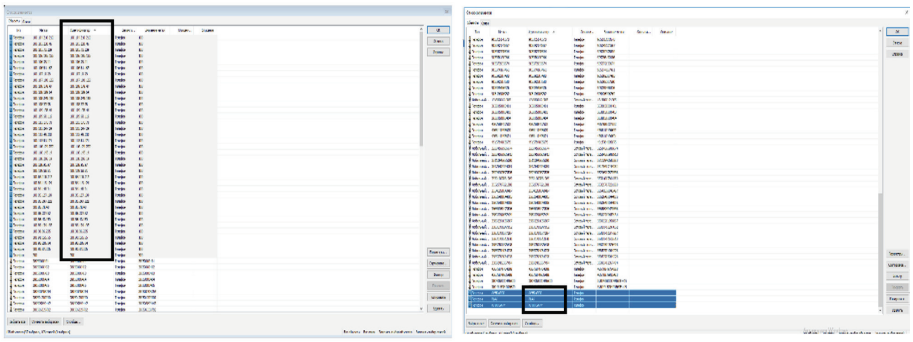
Алгоритм цієї операції:

1. Відкриваємо **«Аналіз» - «Список елементів».**



У відкритому вікні у вкладці **«об'єкти»** сортуємо по стовпчику **«Ідентифікатор»** та відмічаємо всі ідентифікатори (*використовуючи клавіші **«SHIFT»** та **«CTRL»***), які мають вигляд IP-адрес, назви та натискаємо клавішу **«Видалити»**, потім **«ОК»**. *Аналогічним чином можна вибрати сервісні номери оператора зв'язку, при умові, що аналітик впевнений, що вибрані номери телефону належать оператору.*

2. Після цих маніпуляцій із схеми пропадуть вказані вище з'єднання.



Алгоритм визначення активності абонента щодо контактів з іншими. До первинних ознак, котрі характеризують об'єкт, та, які можна дізнатись з білінгу, відносяться:

активність абонента – загальна кількість телефонних з'єднань (скільки їх всього зафіксовано за досліджуваний період);

частота з'єднань – дні пікової активності або періоди затишшя;

кількість зв'язків абонента – зі скількома контактами об'єкт підтримує зв'язок;

середня тривалість розмов – скільки в середньому об'єкт витрачає на розмову (цей показник цікавий для виявлення аномально довгих дзвінків);

використання інтернету (GPRS - з'єднання).

Статистика дзвінків (з'єднань) абонента дозволяє виявити тих абонентів, з якими він підтримує зв'язок. Отримавши ці дані та відсортувавши їх за спаданням, отримуємо перелік контактів фігуранта із зазначенням кількості дзвінків. Цей список можна поділити на три умовні групи:

стабільні – це найчастіші контакти, з якими розмови відбуваються практично щодня або й декілька разів на день (до цієї категорії належать абоненти, з якими об'єкт підтримує постійні контакти, це люди, з якими об'єкт дуже часто спілкується – близькі родичі, найкращі товариші, віддані колеги по роботі);

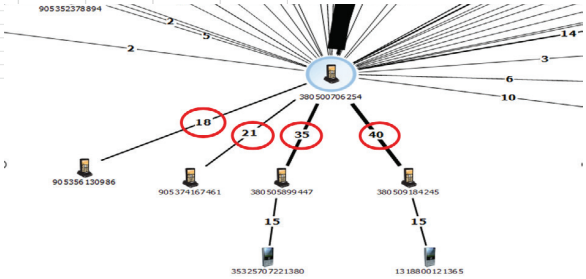
періодичні – це контакти в середній частині списку, з якими розмови відбуваються періодично, не стабільні, але і не одноразові (до цієї категорії належать абоненти, з якими об'єкт спілкується час від часу – це також можуть бути родичі, товариші і колеги по роботі, але не дуже близькі);

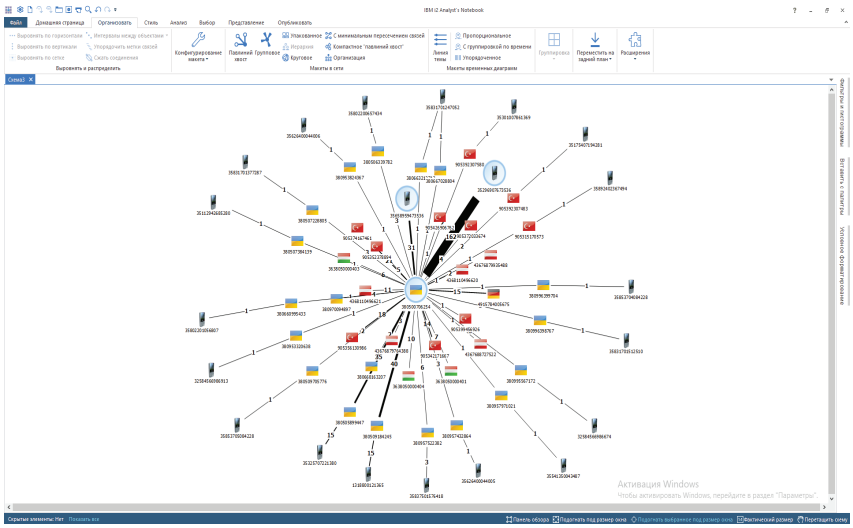
разові – це контакти, з якими відбулось декілька розмов (до цієї категорії належать абоненти, з якими об'єкт мав одноразові справи (сервісні послуги, ремонт, купівля-продаж), консультації, тощо).

Найпростіший спосіб встановлення активних співрозмовників – це у файлі білінгу в нижній частині є поле статистики (*окрім білінгу оператора*) де на кожен номер вказано кількість з'єднань із номером абонента, що досліджується та загальна тривалість спілкування.

325	исх.0	380500706254	380668163207				12.02.2016 16:59	0		
326	вх.SMS	380500706254	38050000403		255011770706254	35296907673536	12.02.2016 17:19	0	Hungary	Hungary
327	==========СТАТИСТИКА==========									
328	вх.	380500706254	905374167461	11	1353					
329	вх.SMS	380500706254	3638050000404	10	0					
330	исх.0	380509184245	380500706254	10	0					
331	вх.SMS	380500706254	700	10	0					
332	исх.	380509184245	380500706254	9	262					
333	вх.	380500706254	380509184245	9	261					
334	исх.0	905374167461	380500706254	9	0					
335	вх.	380500706254	905356130986	8	1110					
336	исх.0	905342171667	380500706254	8	0					
337	GPRS.	380500706254	100.85.137.199	7	14075					
338	вх.	380500706254	4915784005675	7	1038					
339	вх.	380500706254	380505899447	7	569					
340	исх.	380505899447	380500706254	7	568					
341	исх.0	4915784005675	380500706254	7	0					
342	вх.SMS	380500706254	3638050000401	7	0					
343	исх.0	380505899447	380500706254	7	0					
344	исх.0	905356130986	380500706254	7	0					
345	исх.	380500706254	380509184245	6	425					
346	вх.	380509184245	380500706254	6	425					
347	вх.SMS	380500706254	3638050000403	6	0					
348	исх.0	4368110496621	380500706254	6	0					
349	GPRS.	380500706254	100.113.247.24	5	8517					
350	вх.SMS	380500706254	38050000405	5	0					
351	вх.	380500706254	4368110496621	4	636					
352	исх.	380500706254	380505899447	4	486					
353	вх.	380505899447	380500706254	4	486					

На схемі активність абонентів буде вказано вагою зв'язку, а при застосуванні умовного форматування буде відображено товщиною зв'язку, для цього необхідно вибрати *«Стиль» - «Умовне форматування» - «Панель умовного форматування» - «Ширина зв'язку на основі величини транзакції»*, після цієї операції лінії зв'язків збільшаться по товщині пропорційно своєму значенню, після чого можна буде визначити найактивніший зв'язок.





Варто звертати увагу на здійснення дзвінків на номери іноземних операторів. Таким чином, можна встановити країну походження фігуранта або країну призначення, якщо це був незаконний мігрант. Необхідно вибрати через *«Аналіз» - «Список елементів»* виключно номери телефонів, а не IMEI, а потім, використовуючи інструмент *«Стиль» - «Умовне форматування» - «Панель умовного форматування» - «Використати прапори країн для телефонів з кодами виклику»*, натискаючи праву клавішу миші *«Форматувати обрані елементи»*, перевести номери телефонів по кодах країн.

Порядок дослідження білінгу. Досліджуючи відомий факт правопорушення, варто розділити телефонні з'єднання на три стадії:

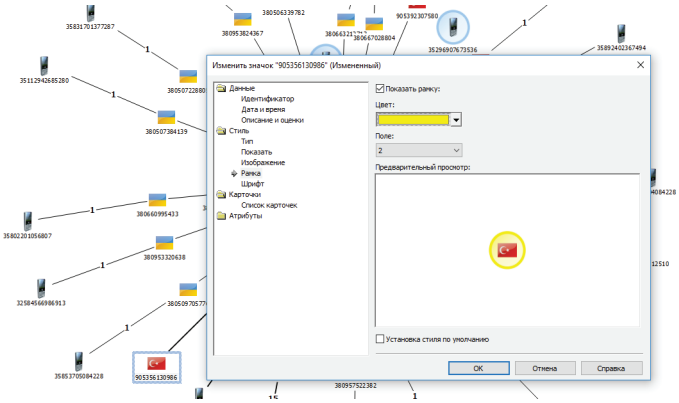
до вчинення правопорушення – на вказаному етапі відбуваються контакти, з абонентами, які залучені до підготовки правопорушення;

період (час) вчинення правопорушення – на вказаному етапі відбуваються контакти, з абонентами, які безпосередньо залучені до правопорушення;

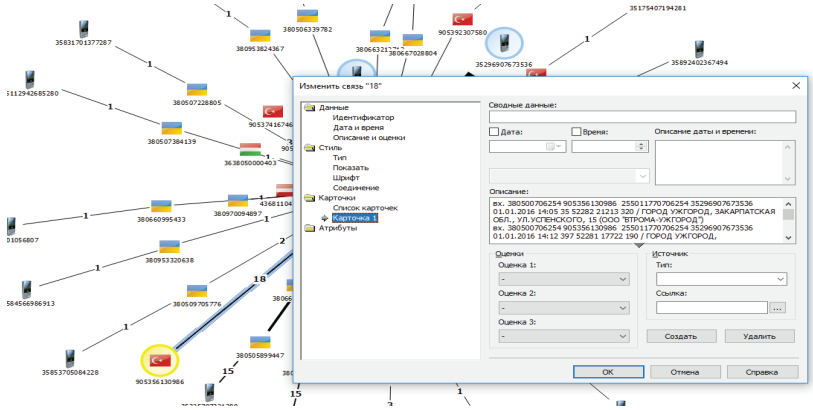
після вчинення правопорушення – у випадку неуспішного здійснення правопорушення на вказаному етапі відбуваються контакти з абонентами, які певною мірою можуть вирішити питання щодо уникнення або полегшення відповідальності за правопорушення.

Основним інструментом цього дослідження буде файл білінга в форматі Microsoft Excel, де місцем дослідження будуть записи необхідного часового проміжку. При встановленні номерів телефонів, які викликають аналітичний та оперативний інтерес, ці номери відмічаються позначками на схемі через властивості об'єкта у вкладці **«Рамка»**.

Відповідно через властивості лінії зв'язку, вкладку **«Карточка»**, можна побачити з'єднання між основним об'єктом та іншим абонентом.



Місце розташування об'єкта та його зв'язку із «цікавим» абонентом має важливе значення, тому важливо усвідомити та переконатись, що досліджуваний телефон має відношення до фігуранта чи події, яка аналізується. Аналізуючи географічні показники розташування базових станцій стільникового зв'язку, можна визначити місця перебування фігуранта та абонентів, з якими він контактував, періоди здійснення поїздок у конкретні райони. Водночас, із географічних показників можна виокремити абонентів, котрі знаходились в оперативно активних регіонах України (*наприклад, при аналізі незаконного переправлення осіб цікавими будуть абоненти, які перебували в місцях тимчасової відсидки мігрантів*).



Крім цього, зазначені відомості можуть становити особливу цінність, коли досліджується конкретний факт правопорушення і необхідно встановити коло осіб, які перебували в цьому районі.

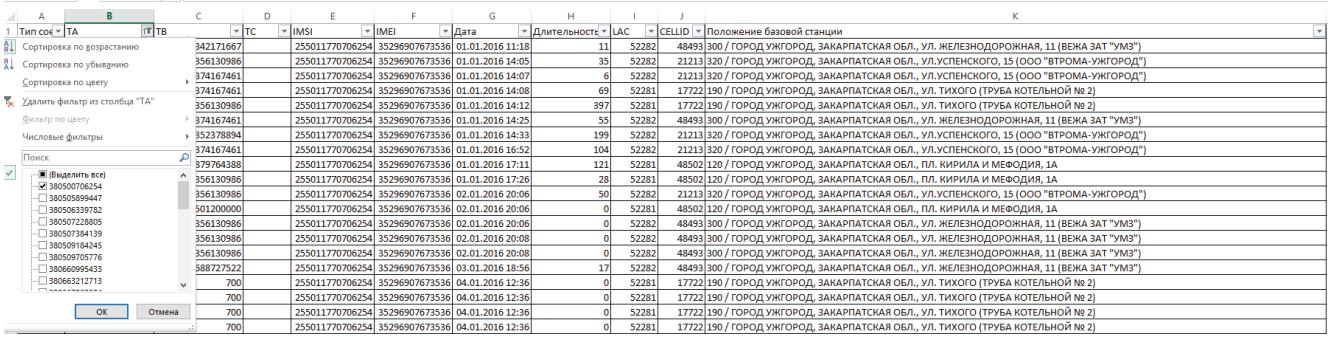
У денний (робочий) період часу можна визначати маршрути пересування абонента та місця, де він зупиняється на тривалий час (можливе місце роботи, навчання, зустрічей). Під час детальних аналізів зручніше позначати відповідні адреси на карті для наочності та ясності.

Алгоритм визначення режиму активності об'єкта. Для встановлення місця проживання фігуранта необхідно аналізувати гарантовано не робочий період часу, переважно з 22:00 до 06:00. У цей проміжок може відбуватись безперервне інтернет-з'єднання, де будуть зазначені базові станції стільникового зв'язку. Іншим шляхом для встановлення місця проживання (ночівлі) є фіксація адрес останнього вечірнього та першого ранкового дзвінка (з'єднання).

З часових показників телефонних з'єднань абонента стільникового зв'язку можна встановити його щоденний розпорядок: час, коли він прокидається та лягає спати; періоди його активності та спокою.

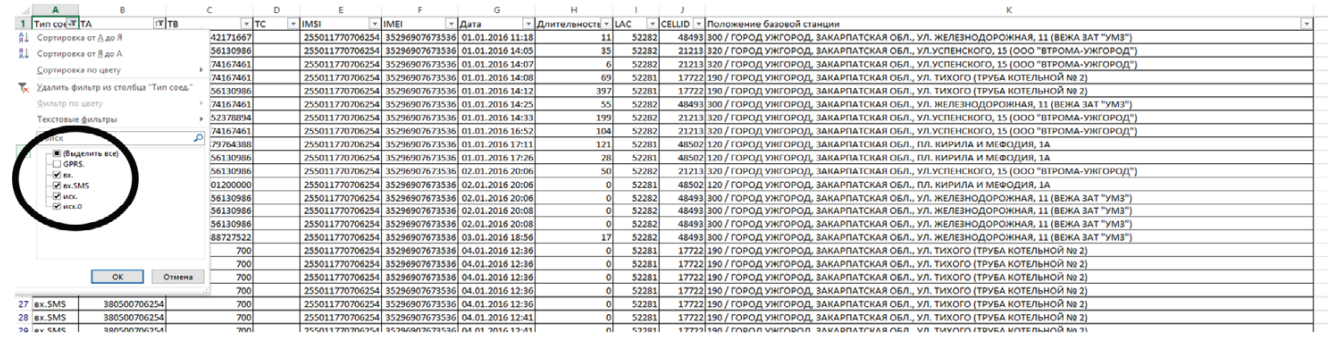
Для цього можна скористатися наступним алгоритмом:

1. У файлі білінгу в графі **«ТА»** виставляємо фільтр (*в білінгі «ТА» цього робити не потрібно*) лише номер телефону об'єкта дослідy.



Тип сое	TA	TB	TC	IMSI	IMEI	Дата	Длительность	LAC	CELLID	Положение базовой станции
	342171667			255011770706254	35296907673536	01.01.2016 11:18	11	52282	48493	300 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ЖЕЛЕЗНОДОРОЖНАЯ, 11 (ВЕЖА ЗАТ "УМЗ")
	356130986			255011770706254	35296907673536	01.01.2016 14:05	35	52282	21213	320 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ.УСПЕНСКОГО, 15 (ООО "ВТРОМА-УЖГОРОД")
	374167461			255011770706254	35296907673536	01.01.2016 14:07	6	52282	21213	320 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ.УСПЕНСКОГО, 15 (ООО "ВТРОМА-УЖГОРОД")
	374167461			255011770706254	35296907673536	01.01.2016 14:08	69	52281	17722	190 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ТИХОГО (ТРУБА КОТЕЛЬНОЙ № 2)
	356130986			255011770706254	35296907673536	01.01.2016 14:12	397	52281	17722	190 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ТИХОГО (ТРУБА КОТЕЛЬНОЙ № 2)
	374167461			255011770706254	35296907673536	01.01.2016 14:25	55	52282	48493	300 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ЖЕЛЕЗНОДОРОЖНАЯ, 11 (ВЕЖА ЗАТ "УМЗ")
	352378894			255011770706254	35296907673536	01.01.2016 14:33	199	52282	21213	320 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ.УСПЕНСКОГО, 15 (ООО "ВТРОМА-УЖГОРОД")
	374167461			255011770706254	35296907673536	01.01.2016 16:52	104	52282	21213	320 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ.УСПЕНСКОГО, 15 (ООО "ВТРОМА-УЖГОРОД")
	379764388			255011770706254	35296907673536	01.01.2016 17:11	121	52281	48502	120 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., ПЛ. КИРИЛА И МЕФОДИЯ, 1А
	356130986			255011770706254	35296907673536	01.01.2016 17:26	28	52281	48502	120 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., ПЛ. КИРИЛА И МЕФОДИЯ, 1А
	356130986			255011770706254	35296907673536	02.01.2016 20:06	50	52282	21213	320 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ.УСПЕНСКОГО, 15 (ООО "ВТРОМА-УЖГОРОД")
	501200000			255011770706254	35296907673536	02.01.2016 20:06	0	52281	48502	120 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., ПЛ. КИРИЛА И МЕФОДИЯ, 1А
	356130986			255011770706254	35296907673536	02.01.2016 20:06	0	52282	48493	300 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ЖЕЛЕЗНОДОРОЖНАЯ, 11 (ВЕЖА ЗАТ "УМЗ")
	356130986			255011770706254	35296907673536	02.01.2016 20:08	0	52282	48493	300 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ЖЕЛЕЗНОДОРОЖНАЯ, 11 (ВЕЖА ЗАТ "УМЗ")
	356130986			255011770706254	35296907673536	02.01.2016 20:08	0	52282	48493	300 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ЖЕЛЕЗНОДОРОЖНАЯ, 11 (ВЕЖА ЗАТ "УМЗ")
	588727522			255011770706254	35296907673536	03.01.2016 18:56	17	52282	48493	300 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ЖЕЛЕЗНОДОРОЖНАЯ, 11 (ВЕЖА ЗАТ "УМЗ")
	700			255011770706254	35296907673536	04.01.2016 12:36	0	52281	17722	190 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ТИХОГО (ТРУБА КОТЕЛЬНОЙ № 2)
	700			255011770706254	35296907673536	04.01.2016 12:36	0	52281	17722	190 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ТИХОГО (ТРУБА КОТЕЛЬНОЙ № 2)
	700			255011770706254	35296907673536	04.01.2016 12:36	0	52281	17722	190 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ТИХОГО (ТРУБА КОТЕЛЬНОЙ № 2)
	700			255011770706254	35296907673536	04.01.2016 12:36	0	52281	17722	190 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ТИХОГО (ТРУБА КОТЕЛЬНОЙ № 2)

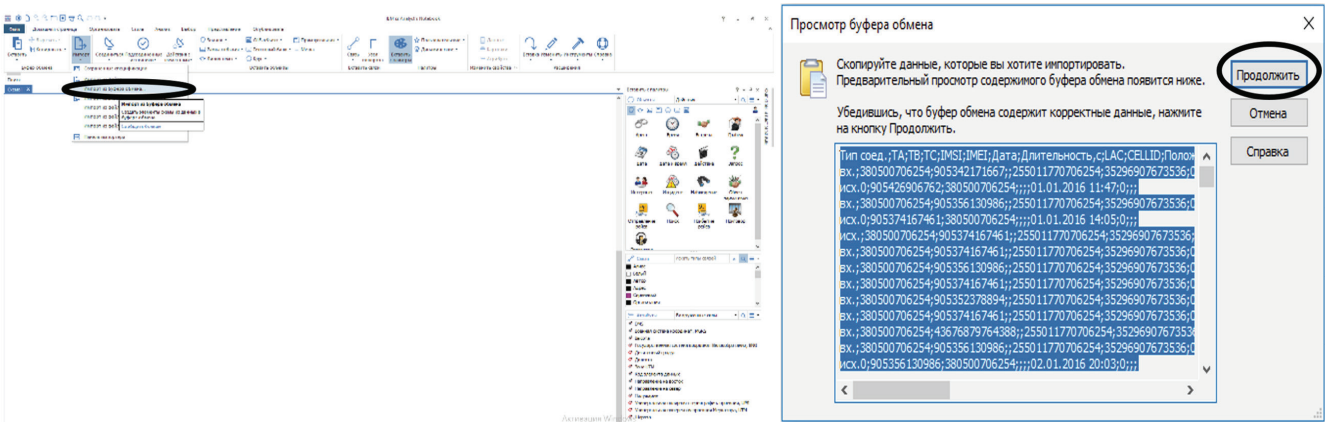
2. У графі **«Тип соед.»** залишаємо лише типи з'єднань **«вх.»** (*вхідний*), **«вих.»** (*вихідний*), **«вх. SMS»** (*вхідна СМС*), **«вих. SMS»** (*вихідна СМС*), **«вих.0»** (*абонент намагався здійснити дзвінок*), тобто ті типи з'єднань коли абонент перебував в активності.



Тип сое	TA	TB	TC	IMSI	IMEI	Дата	Длительность	LAC	CELLID	Положение базовой станции
	42171667			255011770706254	35296907673536	01.01.2016 11:18	11	52282	48493	300 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ЖЕЛЕЗНОДОРОЖНАЯ, 11 (ВЕЖА ЗАТ "УМЗ")
	56130986			255011770706254	35296907673536	01.01.2016 14:05	35	52282	21213	320 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ.УСПЕНСКОГО, 15 (ООО "ВТРОМА-УЖГОРОД")
	74167461			255011770706254	35296907673536	01.01.2016 14:07	6	52282	21213	320 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ.УСПЕНСКОГО, 15 (ООО "ВТРОМА-УЖГОРОД")
	74167461			255011770706254	35296907673536	01.01.2016 14:08	69	52281	17722	190 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ТИХОГО (ТРУБА КОТЕЛЬНОЙ № 2)
	56130986			255011770706254	35296907673536	01.01.2016 14:12	397	52281	17722	190 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ТИХОГО (ТРУБА КОТЕЛЬНОЙ № 2)
	74167461			255011770706254	35296907673536	01.01.2016 14:25	55	52282	48493	300 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ЖЕЛЕЗНОДОРОЖНАЯ, 11 (ВЕЖА ЗАТ "УМЗ")
	52378894			255011770706254	35296907673536	01.01.2016 14:33	199	52282	21213	320 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ.УСПЕНСКОГО, 15 (ООО "ВТРОМА-УЖГОРОД")
	74167461			255011770706254	35296907673536	01.01.2016 16:52	104	52282	21213	320 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ.УСПЕНСКОГО, 15 (ООО "ВТРОМА-УЖГОРОД")
	79764388			255011770706254	35296907673536	01.01.2016 17:11	121	52281	48502	120 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., ПЛ. КИРИЛА И МЕФОДИЯ, 1А
	56130986			255011770706254	35296907673536	01.01.2016 17:26	28	52281	48502	120 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., ПЛ. КИРИЛА И МЕФОДИЯ, 1А
	56130986			255011770706254	35296907673536	02.01.2016 20:06	50	52282	21213	320 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ.УСПЕНСКОГО, 15 (ООО "ВТРОМА-УЖГОРОД")
	01200000			255011770706254	35296907673536	02.01.2016 20:06	0	52281	48502	120 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., ПЛ. КИРИЛА И МЕФОДИЯ, 1А
	56130986			255011770706254	35296907673536	02.01.2016 20:06	0	52282	48493	300 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ЖЕЛЕЗНОДОРОЖНАЯ, 11 (ВЕЖА ЗАТ "УМЗ")
	56130986			255011770706254	35296907673536	02.01.2016 20:08	0	52282	48493	300 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ЖЕЛЕЗНОДОРОЖНАЯ, 11 (ВЕЖА ЗАТ "УМЗ")
	56130986			255011770706254	35296907673536	02.01.2016 20:08	0	52282	48493	300 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ЖЕЛЕЗНОДОРОЖНАЯ, 11 (ВЕЖА ЗАТ "УМЗ")
	88727522			255011770706254	35296907673536	03.01.2016 18:56	17	52282	48493	300 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ЖЕЛЕЗНОДОРОЖНАЯ, 11 (ВЕЖА ЗАТ "УМЗ")
	700			255011770706254	35296907673536	04.01.2016 12:36	0	52281	17722	190 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ТИХОГО (ТРУБА КОТЕЛЬНОЙ № 2)
	700			255011770706254	35296907673536	04.01.2016 12:36	0	52281	17722	190 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ТИХОГО (ТРУБА КОТЕЛЬНОЙ № 2)
	700			255011770706254	35296907673536	04.01.2016 12:36	0	52281	17722	190 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ТИХОГО (ТРУБА КОТЕЛЬНОЙ № 2)
	700			255011770706254	35296907673536	04.01.2016 12:36	0	52281	17722	190 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ТИХОГО (ТРУБА КОТЕЛЬНОЙ № 2)
вх.SMS	380500706254		700	255011770706254	35296907673536	04.01.2016 12:36	0	52281	17722	190 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ТИХОГО (ТРУБА КОТЕЛЬНОЙ № 2)
вх.SMS	380500706254		700	255011770706254	35296907673536	04.01.2016 12:41	0	52281	17722	190 / ГОРОД УЖГОРОД, ЗАКАРПАТСКАЯ ОБЛ., УЛ. ТИХОГО (ТРУБА КОТЕЛЬНОЙ № 2)

3. Виділяємо все **«Ctrl+A»**, копіюємо в буфер обміну **«Ctrl+C»** та починаємо формувати схему в **i2 Analyst`s Notebook.**

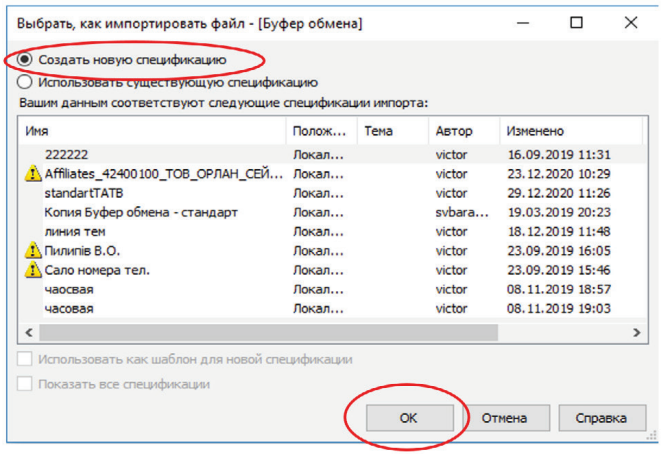
3.1. Відкриваємо **i2 Analyst`s Notebook** вибираємо в меню **«Імпорт»**, **«Імпорт із буфера обміну…»**

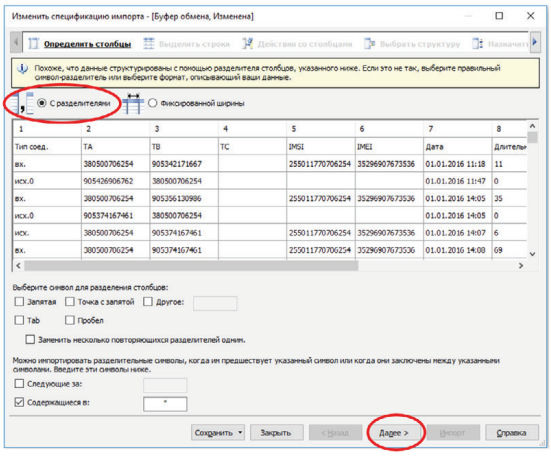


3.2. У вікні натискаємо **«Продовжити»**

3.3. Вибираємо **«Створити нову специфікацію»** та натискаємо **«ОК»**.

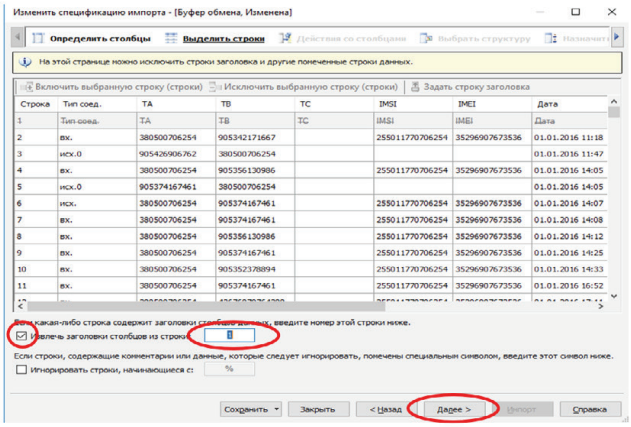
3.4. Запускається майстер створення специфікацій крок 1 – перевіряємо основні налаштування і натискаємо **«Далі»**.

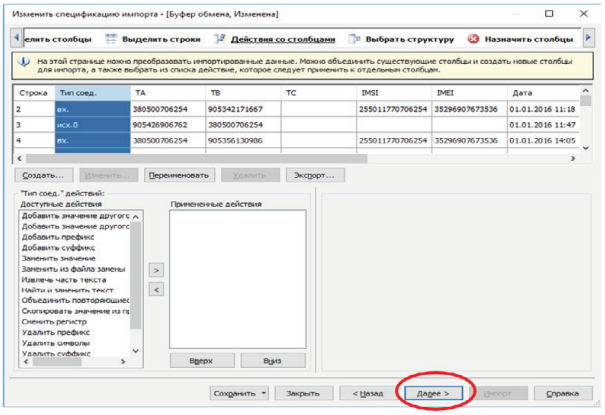




3.5. Визначаємо заголовок та натискаємо **«Далі»**.

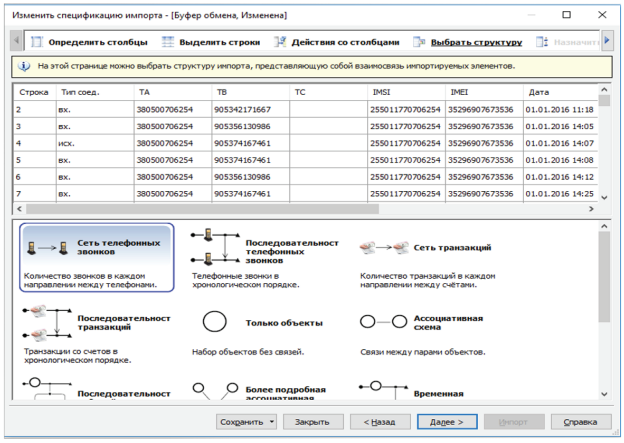
3.6. Якщо нема необхідності доставляти якихось суфіксів та префіксів, то наступний крок натискаємо кнопку **«Далі»**.

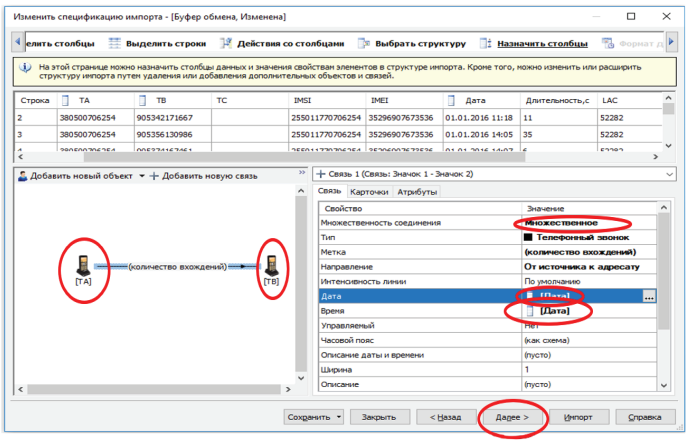




3.7. У вікні вибору структури вибираємо звичайну структуру **«Мережа телефонних дзвінків».**

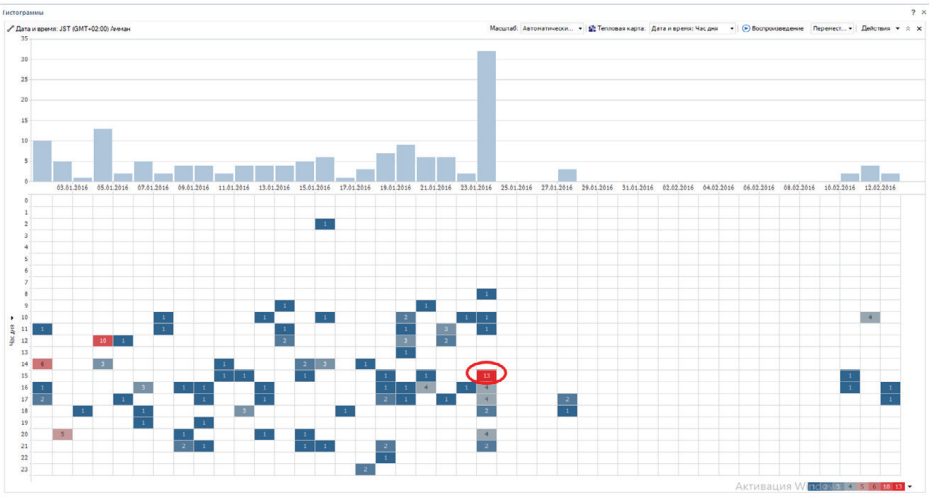
3.8. Отримаємо вікно формування схеми, в якій шляхом перетаскування відповідного стовпчика формується сама схема. На зв'язках встановлюємо: «множинність з'єднань» - «множинний», мітка - «кількість входжень», «Дата» - «Дата», «Час» - «Дата». На об'єктах: абоненти ТА та ТВ. Натискаємо **«Далі».**





3.9. Якщо формат дати не приведений до єдиного формату, в наступному вікні дату приводиться до формату **«dd.MM.yyyy H:mm»** і потім натискається кнопка **«Імпорт».**

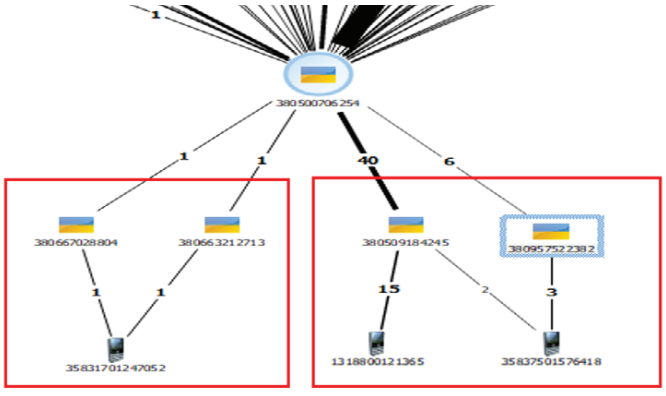
3.10. У подальшому використовується інструмент **«Фільтри и гістограми»** будуються гістограми, на яких видно дні, часи коли був активний абонент. Виходячи з наведеного прикладу видно, що активність припадає на **«23.01.16».**



При виборі інструменту **«Теплова карта»**, наприклад до **«Час дня»** можна побачити години активності, в нашому випадку це з 15.00 по 16.00.

Використовуючи вказані елементи можна побачити різні моменти активності.

Порядок здійснення аналізу терміналів. З аналізу IMEI можна дізнатись, які термінали використовує фігурант, а також встановити ДУОСи – термінали з функцією використання двох сім-карток. У подальшому можна дізнатись інший номер абонента (в т.ч. таємний), який використовується в іншому слоті телефона. Виходячи з досвіду ДУОСи відрізнялись у переважній більшості 7 та 14 цифрою, хоча останнім часом виробники ДУОСів виготовляють термінали, де різниця між слотами сім-карток може бути не тільки на одну цифру, а на декілька. Детальну інформацію про це треба дивитися на технічних описах до кожної конкретної моделі терміналу в мережі INTERNET.



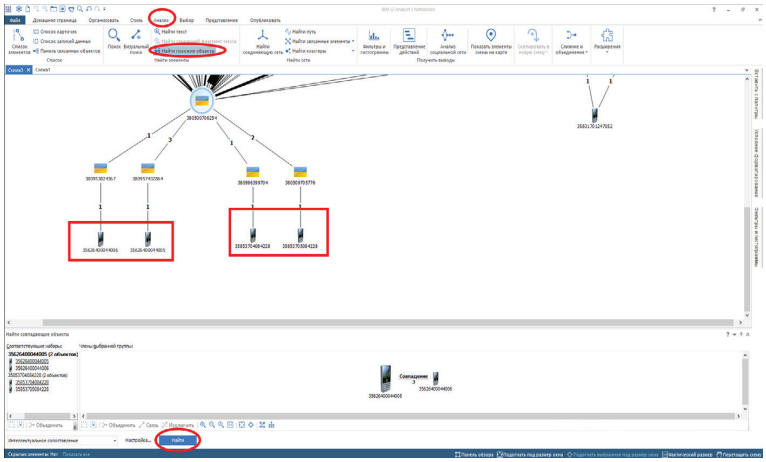
Якщо, будь-який контакт об'єкта під час спілкування (*в періоді дії білінгу*) використовував декілька терміналів, або декілька сім-карток на схемі зав'язків це відображається відповідними з'єднаннями.

Приклад: об'єкт дослідження абонент «380500706254» мав контакти з абонентом «380509184245», який використовував IMEI «1318800121365» та «35837501576418» та контакт з абонентом «380957522382», який використовував IMEI «35837501576418», таким чином можна припустити, що ці номери теле-

фонів та термінали належать одній людині. Абоненти «380667028804» та «380663212713» використовували один і той же термінал, тому також можна припустити, що це належить одній особі.

Один із способів визначення ДУОСів це застосування інструменту **«Аналіз» - «Найти схожі об'єкти».**

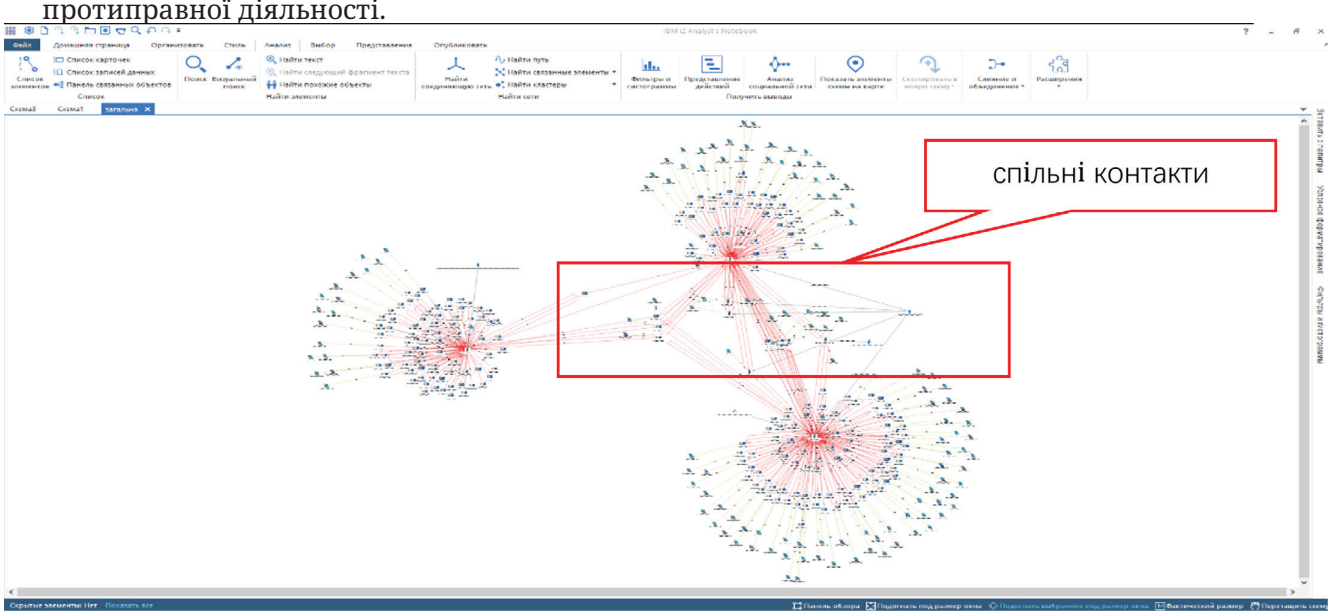
У конкретному випадку є 2 способи виявлення ДУОСів.



Алгоритм здійснення аналізу декількох білінгів. У ході проведення кримінального аналізу найчастіше аналізуються телефонні з'єднання декількох абонентів стільникового зв'язку, які пов'язані між собою та причетні до конкретного або декількох правопорушень на державному кордоні.

Процес поєднання білінгів здійснюється методом з'єднання білінгів за таким алгоритмом:

1. Формуємо окремі схеми файлів білінгів, до прикладу **«Білінг1», «Білінг2», «Білінг3»** (*процес формування описаний вище*).
2. Виділити **«Білінг1»** (*виділяємо все* ***«Ctrl+A»****, копіюємо в буфер обміну* ***«Ctrl+C»*****)**, вставляємо до «Білінг2» (***«Ctrl+V»),*** аналогічно вставляємо «Білінг3». Після цих операцій схема має приблизно наступний вигляд, де, в першу чергу, звертається увага на встановлення спільних контактів, оскільки вони також можуть становити оперативний інтерес і входити до числа пособників протиправної діяльності.



Варто робити акценти на збільшення активності у всіх абонентів чи їх спільне перебування в одному районі. Таким чином можна виявити інші, невідомі раніше правопорушення, до котрих причетні фігуранти аналізу.

Як було зазначено, на початку кожен окремий аналіз має свою мету та завдання, тому й шляхи до їх вирішення будуть мати дещо відмінний і специфічний характер. У будь-якому випадку кримінальний аналітик повинен постійно перебувати в інформаційному контакті з оперативним працівником.

Всі методи, алгоритми описані вище не є догмою, а лише частина аналітичної роботи, яка певним чином полегшує, візуалізує загальний аналітичний процес. Необхідно також враховувати зміни технологічних процесів операторів стільникового зв'язку, інтернет-ресурсів, географічної специфіки, політичної ситуації, оновлень програмного забезпечення та інших різноманітних факторів. Ще раз хотілось би наголосити, що дослідження телефонних з'єднань побудовано на виявленні закономірностей чи, навпаки, відмінностей від щоденного ритму життя абонента.

> *Аналітичне дослідження – це процес творчий, якість дослідження залежить від досвіду, ерудиції, креативності аналітика.*

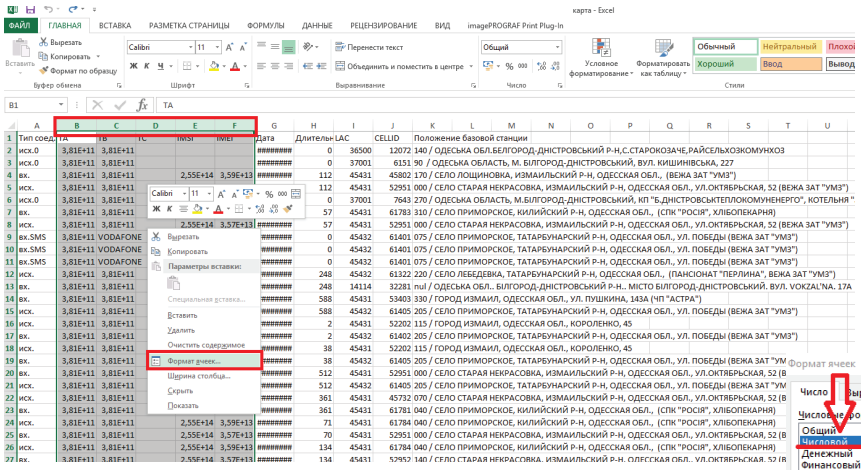
СТВОРЕННЯ СХЕМИ ЗВ`ЯЗКІВ. ВИКОРИСТАННЯ GOOGLE EARTH ТА I2 ANALYST`S NOTEBOOK

Google Earth – це програма в Гугл, в рамках якої в мережі інтернет були викладені супутникові фотографії нашої планети. Головною відмінністю цієї програми від картографічної Google Maps і інших схожих програм – це можливість тривимірного перегляду ландшафту поверхні землі або будівель / споруд. Слід відзначити, що фотографії деяких регіонів мають дуже велике розширення, що дозволяє у найдрібніших деталях розглянути зображення.

У даний момент програма представлена як у безкоштовній, так і платних версіях (платні Google Earth Plus і Google Earth Pro (їх можуть завантажити зареєстровані користувачі), мають підтримку GPS навігації, більшу роздільну здатність при роздруківці фото та більше засобів презентації. Під час аналізу білінгу для створення схеми взаємозв`язків та її відображення аналітики використовують програму «Google Earth» за наступним алгоритмом:

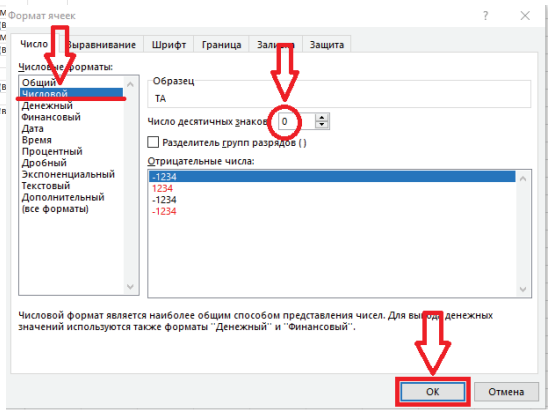
I. Етап: підготовка файлу EXCEL.

1. Дії виконуються в разі надання трафіків типів «ТАТВ» !



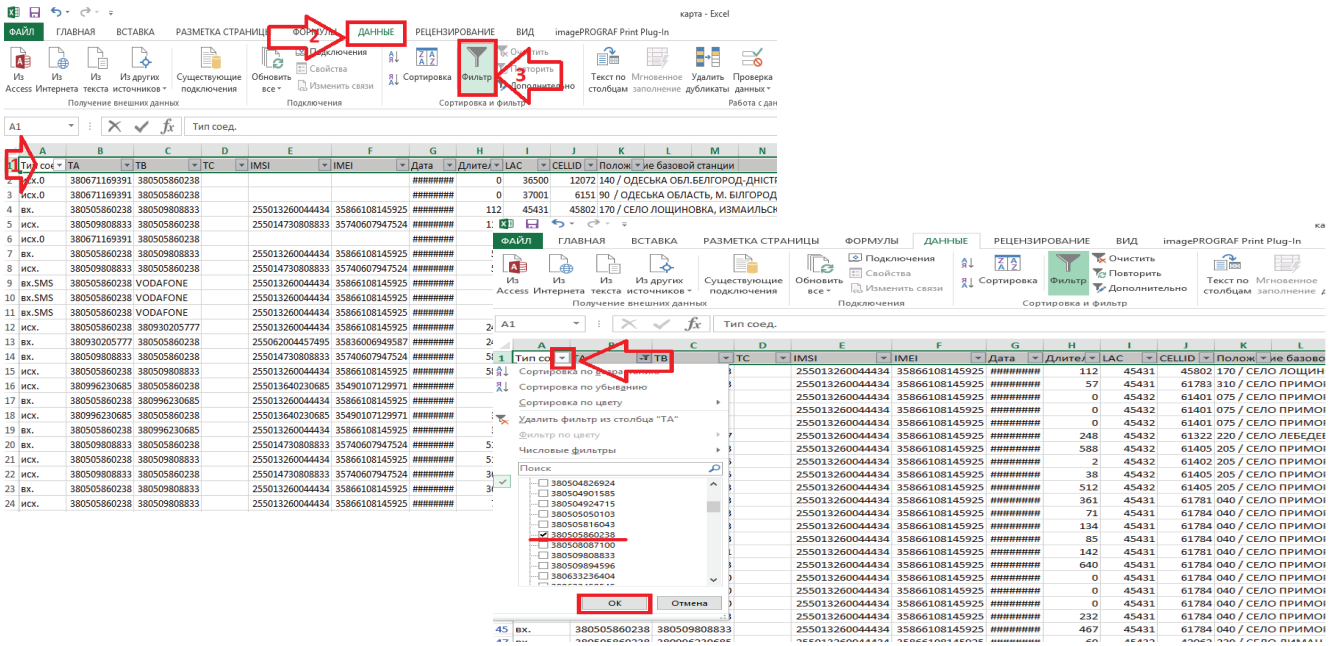
1) Відкриваємо трафік «ТАТВ» в EXCEL виділяємо та змінюємо формат стовпчиків «В», «С», «D», «Е», «F» на «Числовий».

Число знаків після коми «0». Натискаємо «ОК».

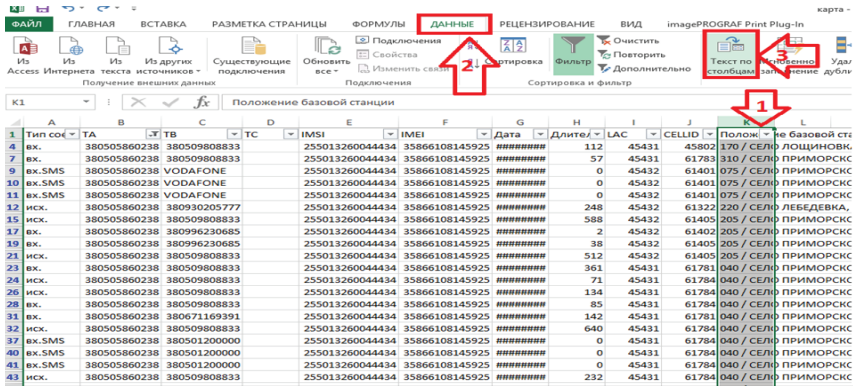


2) Наступним кроком обираємо об'єкти, місцеположення яких потрібно накласти на карту в «Гугл Планеті». Для цього ставимо фільтр на всі стовпчики.

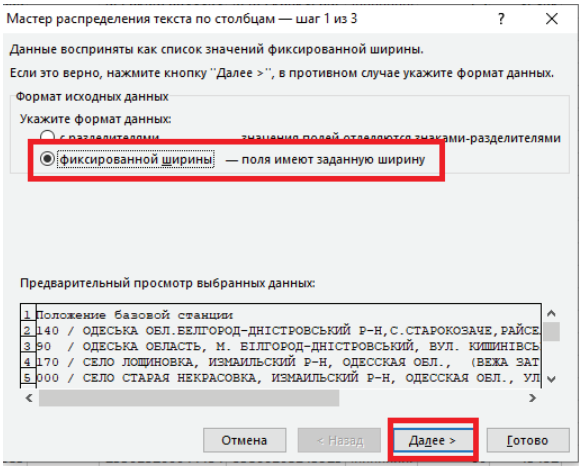
Переходимо у фільтр стовпчика «ТА» та знімаємо позначки з усіх номерів, які нас не цікавлять.



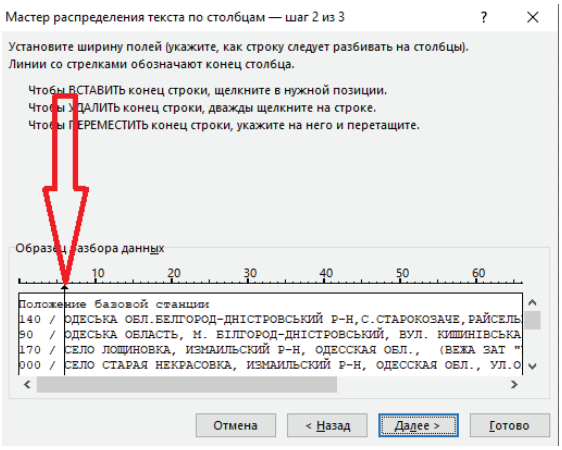
3) Після чого приводимо вигляд стовпчика з назвою «Розташування базової станції» до необхідного. Для цього виділяємо стовпчик «К» та в розділі «Дані» знаходимо та натискаємо на кнопку «Текст по стовпчикам».



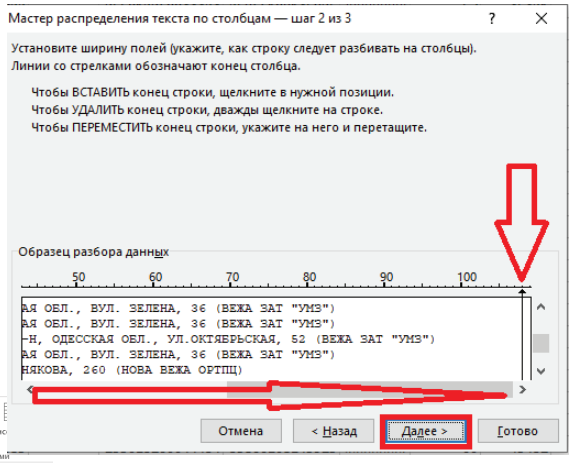
4) У вікні ставимо позначку в полі «Фіксованої ширини», натискаємо «Далі».



5) Наступним кроком задаємо діапазон в якому буде знаходитись адреса базової станції. Для цього перед самим початком адреси виставляємо стрілку, яка буде вказувати початок адреси.

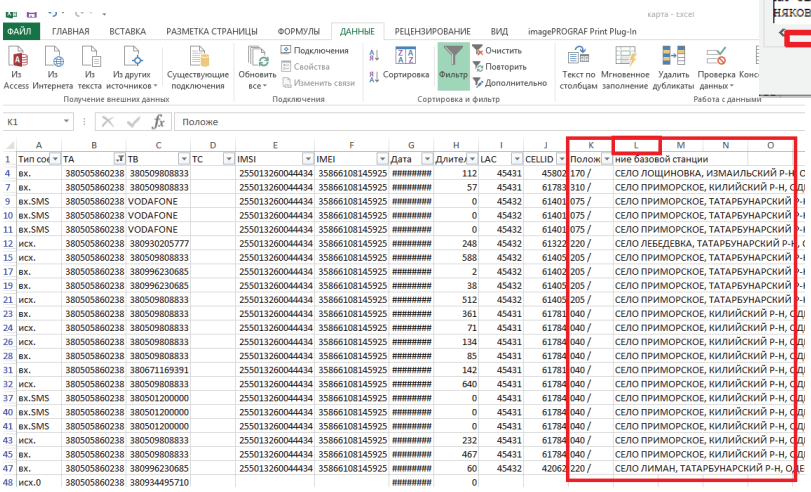


6) У подальшому зверніть увагу на закінчення адреси. Деякі адреси є досить великими, з метою вірного вказання закінчення діапазону перетягуємо данні курсором та виставляємо межі діапазону в кінець (де немає записів).

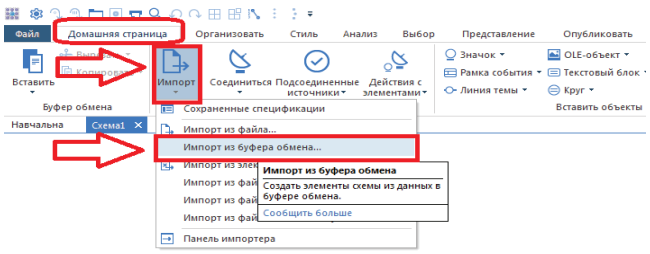


Переміщуємо курсор вниз та перевіряємо чи всі дані знаходяться в діапазоні, якщо ні то переставляємо діапазон. Натискаємо «Далі».

7) Наступне вікно залишаємо без змін та натискаємо «Готово». В результаті проведених дій з'являється стовпчик «L» в якому буде міститися лише адреса базової станції зв'язку.

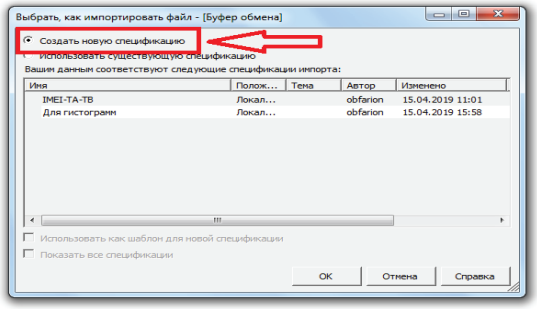


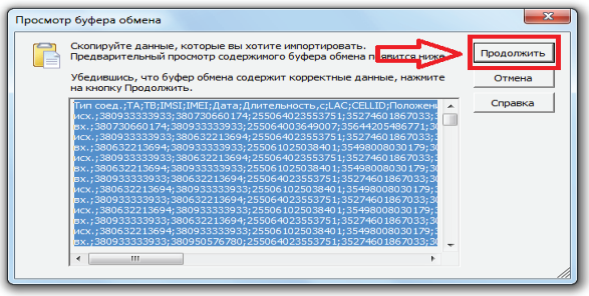
II. Етап: Імпорт з EXCEL в «i2 Analyst`s Notebook» та створення специфікації.



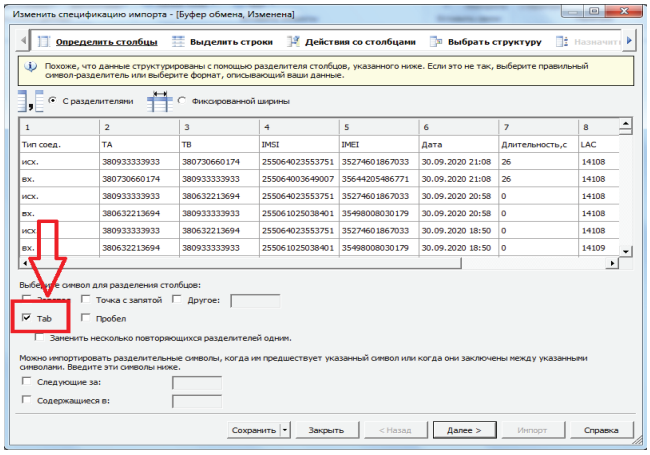
1. Копіюємо всі дані з EXCEL (Наводимо курсор на будь-яку заповнену строку натискаємо CTRL+A потім CTRL+C). Відкриваємо програму «i2 Analyst`s Notebook». На панелі натискаємо **«Домашня сторінка»**, потім натискаємо **«Імпорт»**, у відкритому вікні **«Імпорт із буфера обміну»**.

2. У щойно відкритому вікні натискаємо **«Продовжити»**.

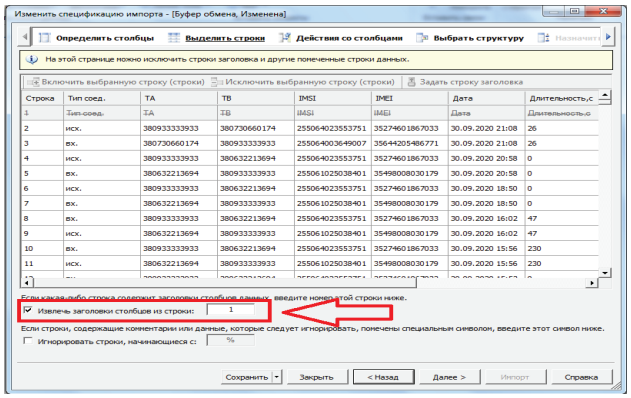




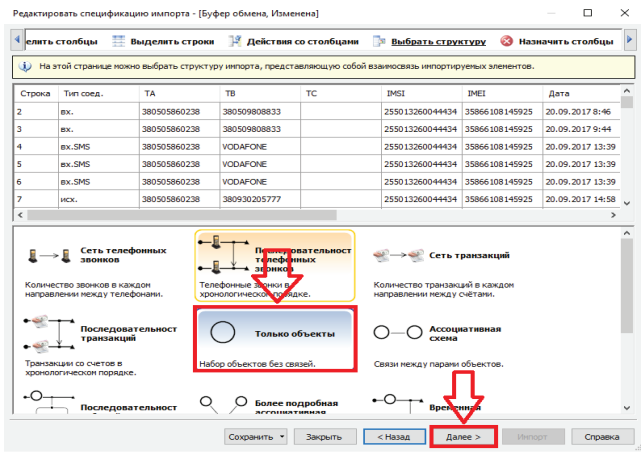
3. Створюємо нову специфікацію. Натискаємо «ОК».



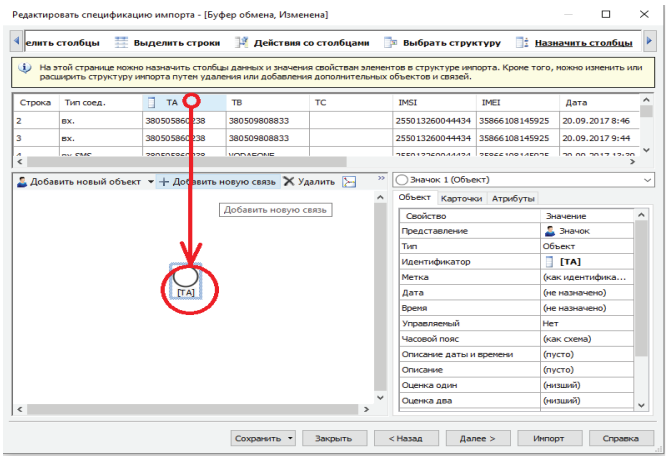
У наступному вікні вибираємо символ для розділення стовпчиків «Tab» та знімаємо відмітки з розділів «Наступні за», «Містяться в». Натискаємо «Далі».



4. На наступній сторінці ставимо відмітку в полі: «Вилучити заголовки із стовпчиків».



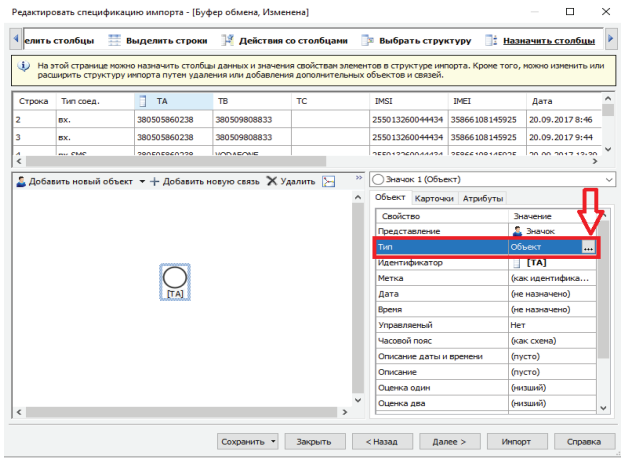
5.Наступну сторінку залишаємо без змін, натискаємо «Далі» та переходимо до розділу «Обрати структуру». На вказаній сторінці обираємо **«Тільки об'єкти»** та натискаємо «Далі».



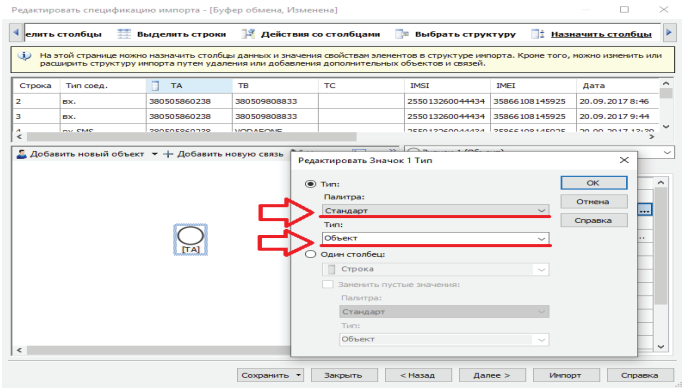
6. У наступному вікні робимо наступні дії:

Наводимо курсор на стовпчик «TA», затискаємо ліву клавішу миші та перетягуємо вказаний стовпчик до кола зображеного на схемі;

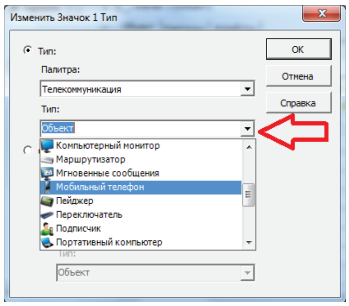
Виконавши вказані дії ми назначимо відповідний ідентифікатор об`єкту.

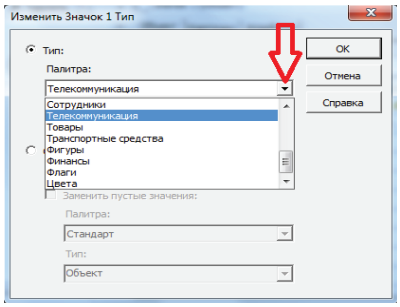


7. За необхідності змінюємо тип об`єкта для цього переходимо в праву частину вікна з написом «Об'єкт». У полі «Тип» - «Об'єкт» натискаємо лівою клавішею миші.



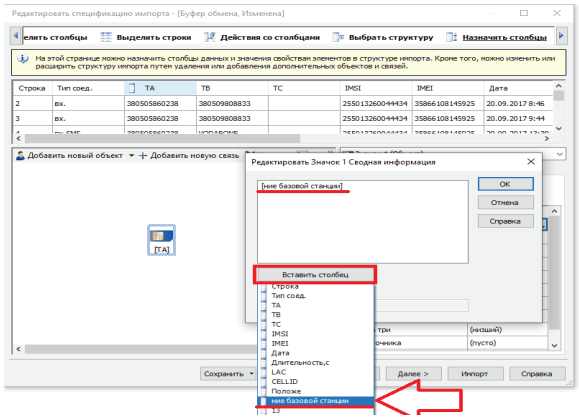
8. У відкритому вікні в розділах «Палітра» та «Тип» обираємо вигляд об`єкта на майбутній схемі наприклад «Мобільний телефон»:

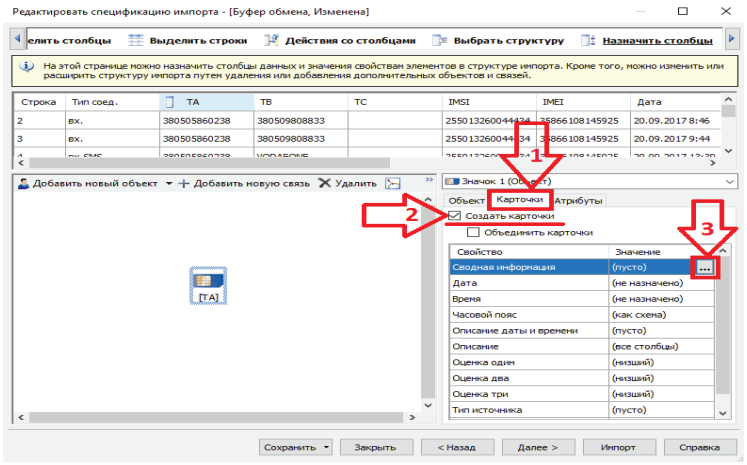




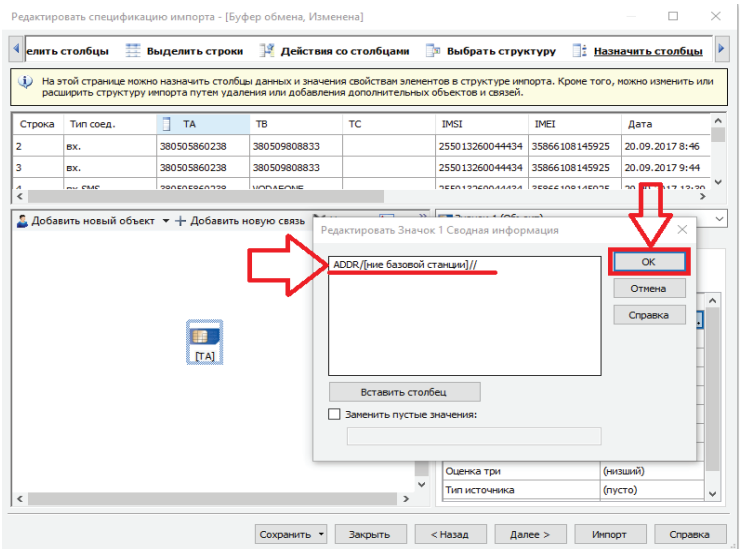
9. Після виконання операцій вносимо інформацію про місцеположення базової станції. Для цього натискаємо на «Карточки» та ставимо відмітку в розділі «Створити карточки». Після чого одразу переходимо до налаштувань «Зведеної інформації».

10. У відкритому вікні натискаємо кнопку «Вставити стовпчик». Вставляємо стовпчик у якому записана адреса базової станції зв'язку.

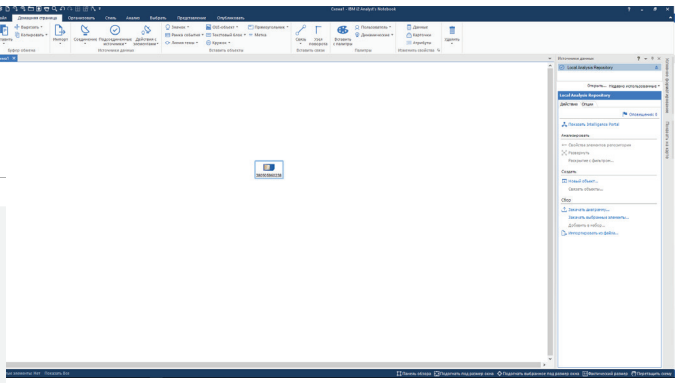


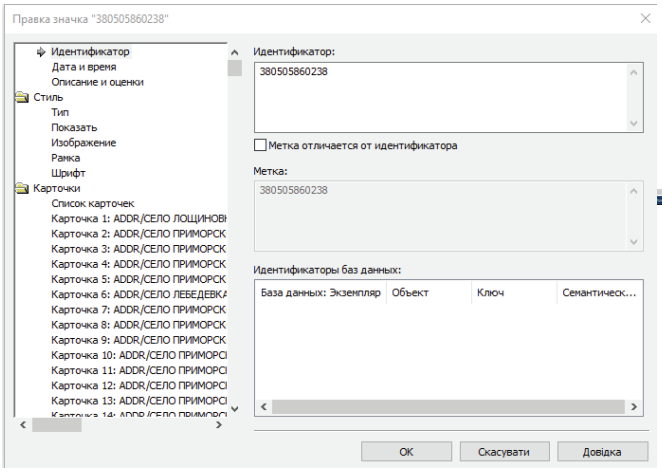


11. **Наступний крок дуже важливий!!!** Англійською мовою, перед назвою стовпчика вводимо вручну: «ADDR/» після назви стовпчика вводимо «//» та натискаємо «ОК». В результаті повинно бути: ADDR/[Розташування базової станції]//



12. Натискаємо кнопку «Імпорт». У результаті, якщо Вами був обраний один номер для відображення його переміщення, на схемі отримаємо одного об'єкта.

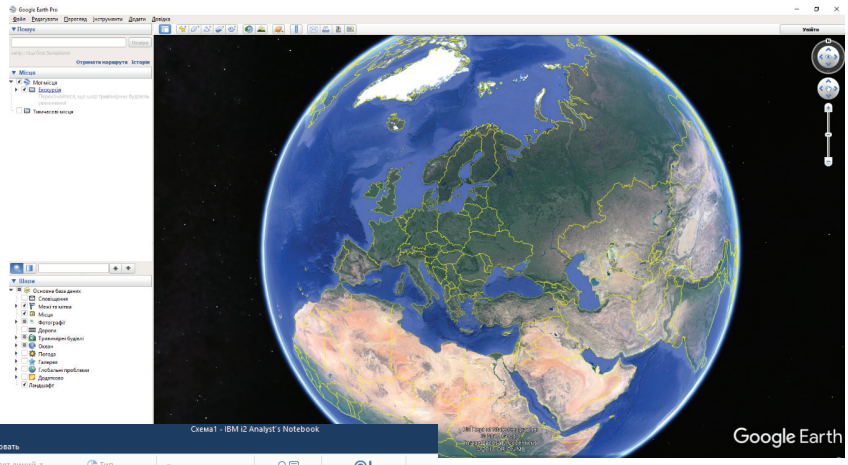


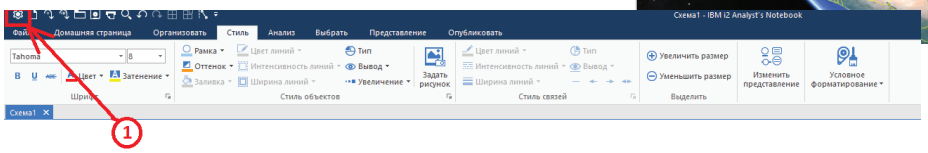


13. Перевіряємо правильність виконаних дій. Для цього подвійним кліком на об'єкт, заходимо в «Правка значка» де зліва знаходимо підрозділ з назвою «Карточки» та в ньому «Список карток». Де бачимо, що місцеположення об'єкта прийняло наступний вигляд.

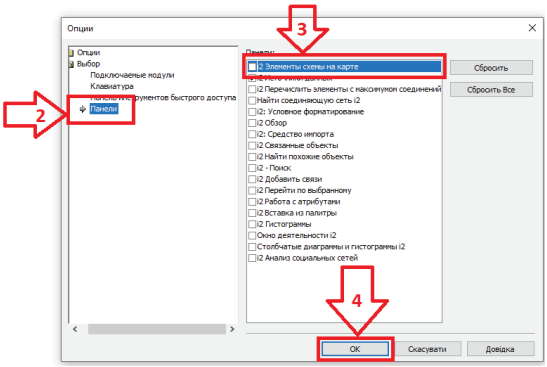
III. Етап: Робота з «Google Earth».

1. Скачуємо та встановлюємо програму «Google Earth». Відкриваємо її та переконуємося, що вона працює.

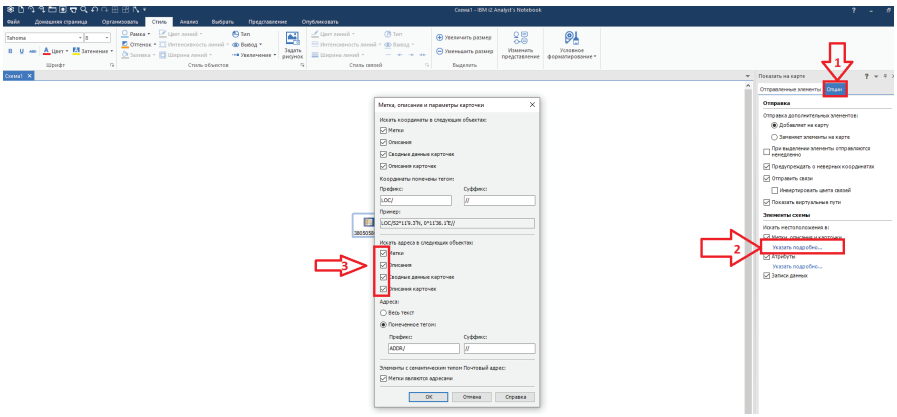


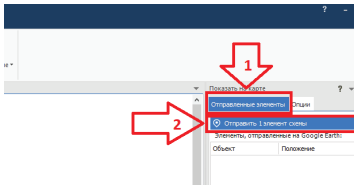


2. Повертаємося до програми « i2 Analyst`s Notebook». В лівому кутку зверху відкриваємо вікно налаштувань. У вікні налаштувань знаходимо та натискаємо розділ «Панелі» в якому ставимо позначку в «i2 Елементи схеми на карті». Після чого натискаємо «ОК».



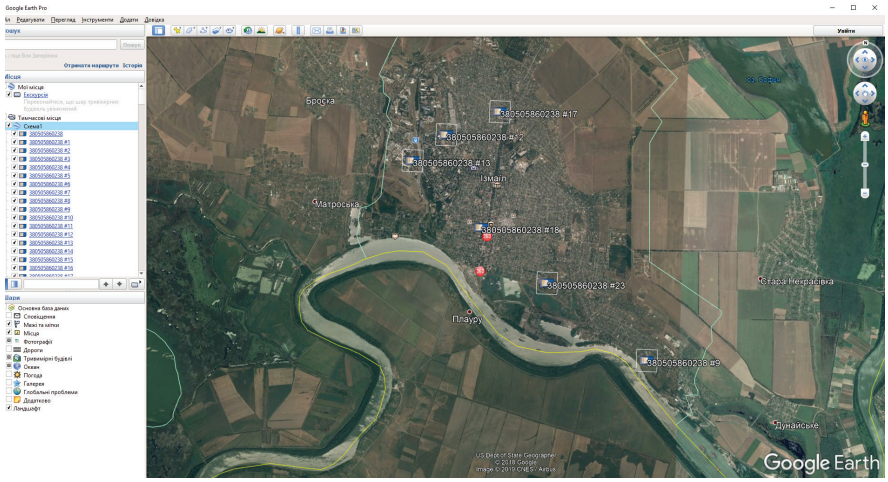
3. З'явилося вікно в якому зверху є розділ «Опції» переходимо в нього. У розділі «Шукати місце розташування в:» під «Мітки, опис и картки» натискаємо на «Вказати детально…». Після чого у відкритому вікні ставимо відмітки у всіх розділах з назвами **«Мітки»**, **«Опис»**, **«Зведені дані карток»**, **«Опис карток»**. Натискаємо «ОК».





4. Наступним кроком переходимо в розділ «**Надіслані елементи**». Натискаємо «**Надіслати елемент схеми**»

5. У результаті в автоматично відкритій програмі «Google Earth» ми маємо змогу бачити місцеположення базових станцій в зоні дії яких перебував об'єкт аналізу.



6. Слід зазначити, що на карту можуть бути перенесені будь-які ідентифікатори, а також фотокартки об'єктів. У розділі зліва з назвою «Тимчасові місця» отримуємо всі послідовно розміщені картки об'єкта аналізу.

DOI: https://doi.org/10.36486/978-966-2310-66-5-30

Технології – це всього лише інструмент

Білл Гейтс

РОЗДІЛ 30
Аналіз та операції з великими даними в середовищі R

Микола Карчевський

Про R. R - це мова програмування і програмне середовище (RStudio) для статистичних обчислень, аналізу та візуалізації даних, має широкий набір функцій, які дозволяють швидко і легко опрацьовувати великі масиви даних [1].

R була створена в 1993 році Россом Іхакою та Робертом Джентлменом, працівниками Оклендського Університету в Новій Зеландії. Іхака і Джентлмен були незадоволені наявними мовами програмування для статистичного аналізу. Вони вважали, що ці мови є занадто складними для навчання і використання, а також не пропонують достатнього рівня гнучкості.

> *R була розроблена як спроба створити мову програмування, яка була б простішою в освоєнні, але в той же час пропонувала б потужний набір функцій для статистичного аналізу.*

Назва R походить від перших літер імен її розробників.

R може використовуватися для виконання широкого спектра завдань, включаючи:

збір і підготовку даних
описову статистику
перевірку гіпотез
регресію
кластеризацію
машинне навчання

R має ліцензію GNU General Public License, що дозволяє вільно використовувати, розповсюджувати та модифікувати мову.

R vs. Python. Це обидві мови програмування з відкритим кодом, які широко використовуються для статистичного аналізу. Однак між ними є деякі ключові відмінності. Розробники професійної сертифікаційної програми «Аналіз даних від Google» систематизують ці відмінності наступним чином [2]

Мови	R	Python
Спільні риси	- відкритий вихідний код - дані зберігаються у датафреймах - формули та функції легко використовувати - інтернет-спільнота для розробки коду та консультативної підтримки	- відкритий вихідний код - дані зберігаються у датафреймах - формули та функції легко використовувати - інтернет-спільнота для розробки коду та консультативної підтримки
Переваги	- бібліотеки та пакети для маніпуляцій з даними, їх візуалізації, статистичних операцій *- «скальпельний» підхід до даних: існують спеціалізовані пакети (packages), для різноманітних завдань щодо обробки даних*	- простий синтаксис для потреб машинного навчання - інтегрується з хмарними платформами, такими як Google Cloud, веб-сервісами Amazon і Azure
Виклики	- неповні угоди про найменування ускладнюють для початківців вибір правильних функцій - методи обробки змінних можуть бути складними для розуміння початківцями	- багато різноманітних рішень для початківців щодо введення/виведення даних, структури, змінних, пакетів і об'єктів *- підхід «швейцарського ножа» для даних: необхідно визначати спосіб бажаних дій з даними*

Таким чином, *основна різниця між R та Python полягає в тому, що R - це мова програмування, орієнтована на статистику, тоді як Python - мова програмування загального призначення.*

Корисні посилання

The R Project for Statistical Computing: офіційний сайт для завантаження R та документації. https://www.r-project.org/

R Manuals: посилання на документи та інструкції з використання від команди розробників. https://cran.r-project.org/manuals.html

Coding Club R Tutorials: набір навчальних вправ з R. https://ourcodingclub.github.io/tutorials.html

R for Beginners: інструкція для початкі роботи з даними, аналізом, статистикою та візуалізацією в R. https://cran.r-project.org/doc/contrib/Paradis-rdebuts_en.pdf

ПРАКТИЧНИЙ КЕЙС

Порівняти кількість облікованих у 2021 та 2022 роках кримінальних проваджень за ознаками крадіжки (ст. 185 КК). Представити у вигляді інтерактивної картограми регіональний розподіл таких проваджень.

Особливості виконання практичного кейсу

Для того, щоб читачі мали можливість працювати над практичним кейсом разом з авторами посібнику, пропонуємо скопіювати вміст створеного нами репозиторію з вхідними даними, скриптами та візуалізаціями [3] у окрему теку, встановити R та RStudio, запустити проєкт R_case.

Також є можливість використовувати хмарний сервіс PositCloud та представлений у відкритому доступі проєкт даного практичного кейсу [4]

Перехід до репозиторію GitHub

Перехід до проєкту у он-лайн середовищі RStudio Posit Cloud

Вхідні дані. Для виконання завдання використаємо базу даних отриману в процесі розробки веб-застосунку «Протидія злочинності в Україні: інфографіка» [5]. Вона міститься у файлі crimes_ukr-REG.RData репозиторію практичного кейсу. Отже, почнемо з завантаження цього файлу (рис. 30.1)

```
1  # Заванаження необхідної бази даних
2  load ("crimes_ukr-REG.RData")
```

Рисунок 30.1. Скрипт завантаження БД

Результатом його виконання стане завантаження у середовище R двох датафреймів (data.frame): crimes_Reg та crimes_Reg_f1 (рис. 30.2).

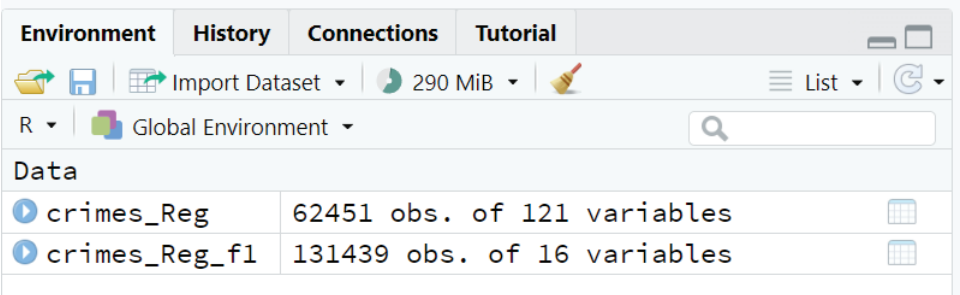


Рисунок 30.2. У середовище R завантажено 2 датафрейми

Перший містить інформацію щодо засуджених осіб, другий – щодо облікованих проваджень. Виходячи з умов кейсу, працюватимемо далі з фреймом crimes_Reg_f1.

Ознайомлювальний аналіз даних. Щоб отримати уявлення про структуру та зміст об'єктів типу data.frame в R, можна використовувати такі команди:

str() - *виводить структуру об'єкта, включаючи назви стовпців, типи даних та кількість спостережень;*
summary() - *виводить статистичний звіт про дані, включаючи середнє, стандартне відхилення, мінімальне та максимальне значення;*
head() та tail() - *виводять перші або останні кілька рядків об'єкта;*
dim() - *виводить кількість стовпців та рядків об'єкта;*
names() - *виводить список назв стовпців об'єкта;*
class() - *виводить тип даних об'єкта.*

Виконання у консолі середовища команди str (crimes_Reg_f1) дозволить отримати уявлення про: кількість спостережень (рядків) та кількість параметрів (стовбців) у датафреймі, який нас цікавить, типи даних у стовбцях, назви стовбців, зміст даних (рис. 30.3).

Отримання даних для візуалізації. Виходячи з умов кейсу, необхідно отримати дані щодо кримінальних проваджень, облікованих за ознаками кримінального правопорушення, передбаченого ст. 185 КК, у 2021 або 2022 році, з урахуванням регіонального розподілу. Отже, з датафрейму crimes_Reg_f1 необхідно отримати данні, що відносяться до 2021 або 2022 року (Year), стосуються статті 185 КК (Article), характеризують облікові провадження (ACC [6]) та адміністративно-територіальний регіон (Region).

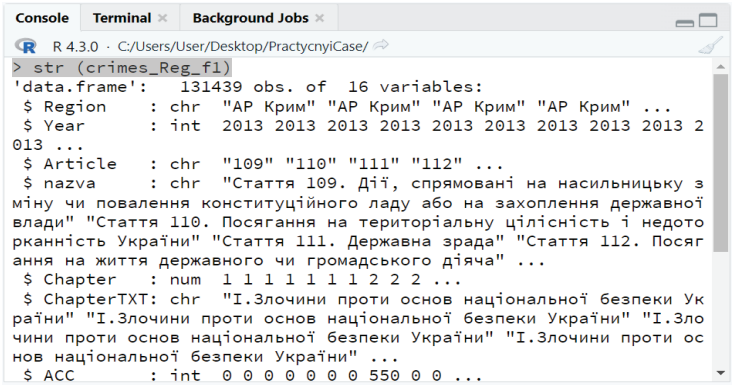


Рисунок 30.3. Оцінка структури та змісту датафрейму за допомогою команди str()

Скористаємося для цього функціями select та subset. Дані функції включені до пакету tidyverse [7], тому підключимо його використовуючи команду library () (рис. 30.4).

```
4  # Підключення бібліотеки
5  library (tidyverse)
```

Рисунок 30.4. Скрипт підключення бібліотеки

Функція select() використовується для вибору стовпців з об'єкта типу data.frame. Функція приймає як аргументи список назв стовпців, які потрібно вибрати.

Функція subset() використовується для вибору рядків або стовпців з об'єкта типу data.frame за певною умовою. Функція приймає як аргументи список умов, які потрібно задовольнити для вибору рядків або стовпців.

Для того, щоб отримати набір даних, який відповідає умовам практичного кейсу необхідно додати до скрипту такі команди (рис. 30.5):

```
7  # Створення датафрейму для візуалізації
8  data<-select(crimes_Reg_f1, c("Year","Region","Article","ACC"))
9  data<-subset(data,(Year>2020&Article=="185"))
10
11 data<-subset(data,!str_detect(Region,"залізниця"))
```

Рисунок 30.5. Скрипт створення data.frame.

У такий спосіб створюється новий датафрейм data. З використанням команди select до нього було включено тільки стовбці з даними про рік обліку, регіон, статтю КК, та кількість облікованих порушень. Далі, використовуючи команду subset у data було залишено тільки ті рядки, що мають відношення до 2021 або 2022 року та стосуються тільки ст. 185 КК.

Якщо переглянути отриманий набір даних, можна побачити, що він містить записи, які відносяться до обліку правопорушень на залізницях, рядки із значенням «Донецька залізниця», «Львівська залізниця», «Одеська залізниця», «Південна залізниця», «Південно-західна залізниця», «Придніпровська залізниця» у полі Region. Для того, щоб вилучити ці записи доповнимо скрипт командою data<-subset(data,!str_detect(Region,»залізниця»))

Вже відома функція subset(), але в якості умови результат функції str_detect(). Остання використовується для виявлення шаблону в рядку, вона повертає логічний вектор із значенням TRUE для кожного елемента рядка, який відповідає шаблону, і FALSE в іншому випадку.

> *У R вектор - це одновимірний об'єкт, який містить ряд значень, які можуть бути одного або різних типів. Вектори можна використовувати для зберігання даних, таких як числа, текст або логічні значення*

Використаємо перед цією функцією оператор !. В R він є логічним, означає заперечення, повертає логічну змінну, яка є протилежною до логічної змінної, яка розташована за ним. Таким чином, отримали умову на підставі якої до data будуть включені тільки записи

```
9  # Приведення назв регіонів у базі географічних даних
10 # у відповідність із назвами у базі статистичних даних
11 shape_data$ADM1_UA <- replace(shape_data$ADM1_UA,
12   shape_data$ADM1_UA == "Автономна Республіка Крим", "АР Крим")
```

Рисунок 30.12. Скрипт зміни значень

в яких поле Region не містить слова «залізниця», іншими словами, тільки дані щодо областей, а також міст Києва та Севастополя,.

Перша візуалізація. Побудуємо візуалізацію отриманих даних у вигляді стовпчикової діаграми. Нехай по осі аргументів будуть розташовані адміністративно-територіальні одиниці, вісь результатів характеризуватиме кількість облікованих проваджень, а дані 2021 та 2022 року будуть представлені у двох окремих сюжетах візуалізації (рис. 30.6).

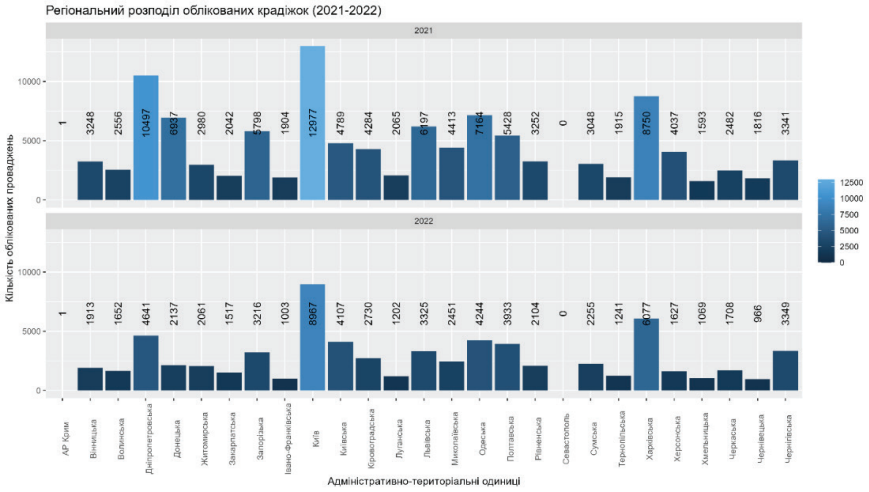


Рисунок 30.6. Візуалізація отриманих даних у вигляді стовпчикової діаграми

Таку візуалізацію було отримано в результаті виконання наступних команд (рис. 30.7):

```
13 # Побудова візуалізації
14 vis1<-ggplot(data,
15               mapping = aes(x=Region, y=ACC, fill=ACC, label=ACC))+
16   geom_bar(stat = "identity")+
17   facet_wrap(.~Year, ncol=1)+
18   theme(legend.title = element_blank(),
19       axis.text.x=element_text(angle = 90))+
20   geom_text(aes(angle=90,y=max(data$ACC/2)))+
21   ggtitle ("Регіональний розподіл облікованих крадіжок (2021-2022)")+
22   ylab ("Кількість облікованих проваджень")+
23   xlab ("Адміністративно-територіальні одиниці")
24
25 # Виведення візуалізації у вікно Viewer
26 vis1
27
28 # Збереження візуалізації у файл
29 ggsave (filename = "diagram.png",vis1,
30         width = 32, height = 18, dpi = 300, units = "cm")
```

Рисунок 30.7. Скрипт візуалізації даних у вигляді стовпчикової діаграми

Прокоментуємо дану частину скрипту. Функція ggplot() є основою пакету tidyverse для візуалізації даних. Вона використовується для створення графіків шляхом поєднання різних компонентів, таких як дані, естетика, геометричні об'єкти та написи.

Результат роботи функції ggplot присвоєно змінній vis1 (рис. 30.7, рядок 14, vis1 <- ggplot…), в нашому випадку це зроблено для того, щоб зберегти побудовану візуалізацію у вигляді графічного файлу.

Джерело даних, осі аргументів та результатів, колір діаграми та зміст підписів визначено у наступній частині: «ggplot(data, mapping = aes(x=Region, y=ACC, fill=ACC, label=ACC))» (рис. 30.7, рядки 14 та 15). Як можна побачити, джерелом даних визначається створений раніше датафрейм data. Естетика (**aes**) діаграми характеризується: 1) змінними для осі x, які містить поле Region (назви адміністративно-територіальних одиниць); 2) змінними для осі y, які містить поле ACC (кількість облікованих проваджень); 3) кольором заповнення елементів діаграми та підписами, які визначаються кількістю облікованих проваджень (fill=ACC, label=ACC).

Команда «geom_bar(stat = "identity")» (рис. 30.7, рядок 16) визначає форму візуалізації як стовпчикову діаграму.

Визначення двох сюжетів за роками спостереження забезпечується командою «facet_wrap(.~Year, ncol=1)» (рис. 30.7, рядок 17).

Налаштування «theme(legend.title = element_blank(), axis.text.x=element_text(angle = 90))» (рис. 30.7, рядки 18 та 19) встановлює, що підпис легенди відсутній (в даному випадку він був би збитковою інформацією), а підписи по горизонтальній осі слід повернути на 90 градусів.

Команда «geom_text(aes(angle=90,y=max(data$ACC/2)))» (рис. 30.7, рядок 20) забезпечує вертикальне розміщення підписів даних на рівні середини максимального значення досліджуваного показника (ACC).

Блок команд «ggtitle («Регіональний розподіл облікованих крадіжок (2021-2022)») + ylab («Кількість облікованих проваджень») + xlab («Адміністративно-територіальні одиниці»)» (рис. 30.7, рядки 21-23) визначає заголовок діаграми, підписи вертикальної та горизонтальної осей.

Команда vis1 забезпечує виведення візуалізації у вікні Plots (рис. 30.7, рядок 26).

Нарешті, збереження отриманої візуалізації у файл «diagram1.png» забезпечується командою «ggsave (filename = "diagram1.png",vis1, width = 32, height = 18, dpi = 300, units = "cm")» (рис. 30.7, рядки 29 та 30). Як можна побачити, аргументами функції ggsave виступають ім'я файлу, змінна, яка містить створену візуалізацію (vis1), розміри візуалізації, одиниці вимірювання, якість графіки.

Повний скрипт для розв'язання цієї частини кейсу представлено у файлі vis1.R репозиторію R_case.

Картограма. Для побудови картограми будемо використовувати бібліотеки leaflet [8], sf [9] та htmlwidgets [10] (рис. 30.8).

```
1  # Підключення бібліотек
2  library (leaflet)
3  library (sf)
4  library (htmlwidgets)
```

Рисунок 30.8. Застосовувані біліотеки

Отримання даних. Географічні дані про межі областей, міст Києва та Севастополя отримаємо з сайту The Humanitarian Data Exchange, що є ресурсом відкритих даних Офісу ООН з координації гуманітарних питань [11]. Копії отриманих з цього ресурсу файлів розміщено нами у теці Shape_files репозиторію практичного кейсу. У датафреймі shape_data збережемо отримані географічні дані використовуючи спеціальну функцію read_sf() (рис. 30.9, рядок 7).

```
6  # Отримання геоданих
7  shape_data <- st_read("Shape_files/ukr_admbnda_adm1_sspe_20230201.shp")
```

Рисунок 30.9. Скрипт збереження географічних даних

Цілком очевидно, що для побудови картограми необхідно буде об'єднати географічні (shape_data) та статистичні дані (data). Спільними полями використовуваних у проєкті датафреймів є поле Region датафрейму data та поле ADM1_UA датафрейму shape_data. Кожне з цих полей містить назви адміністративно-територіальних одиниць. Отже, для коректного об'єднання географічних та статистичних даних необхідно, щоб поля data$Region та shape_data$ADM1_UA містили однакові назви адміністративно-територіальних одиниць.

Для здійснення перевірки використаємо функцію setdiff(), яка порівнює два вектори по елементах. Для кожного елемента першого вектора перевіряється, чи він є в другому векторі. Якщо елемент відсутній в другому векторі, він додається до вектору, який буде повернуто як результат. Виконання в консолі відповідної команди показало, що найменування «АР Крим» присутнє тільки у полі data$Region (рис. 30. 10).

```
> setdiff(data$Region,shape_data$ADM1_UA)
[1] "АР Крим"
```

Рисунок 30.10. Перевірка відповідності даних

Далі дізнаємося, які унікальні значення містить поле найменувань датафрейму з географічними даними. Використаємо для цього функцію unique(). Так само виконаємо її в консолі (рис. 30.11)

Як можна побачити, якщо у датафреймі географічних даних використовується значення «Автономна Республіка Крим», то у датафреймі статистичних даних використовується значення «АР Крим». Використовуючи функцію replace() здійснимо необхідні зміни у shape_data (рис. 30.12, рядки 11 та 12).

```
> setdiff(data$Region,shape_data$ADM1_UA)
[1] "АР Крим"
> unique(shape_data$ADM1_UA)
 [1] "Автономна Республіка Крим" "Черкаська"
 [3] "Чернігівська"               "Чернівецька"
 [5] "Дніпропетровська"           "Донецька"
 [7] "Івано-Франківська"          "Харківська"
 [9] "Херсонська"                 "Хмельницька"
[11] "Кіровоградська"             "Київ"
[13] "Київська"                   "Луганська"
[15] "Львівська"                  "Миколаївська"
[17] "Одеська"                    "Полтавська"
[19] "Рівненська"                 "Севастополь"
[21] "Сумська"                    "Тернопільська"
[23] "Вінницька"                  "Волинська"
[25] "Закарпатська"               "Запорізька"
[27] "Житомирська"
>
```

Рисунок 30.11. Скрипт перевірки унікальних значень, що містить поле найменувань датафрейму з географічними даними

Функція replace() призначена для заміни значень в векторі. В нашому випадку вона використовується з трьома аргументами:

1) shape_data$ADM1_UA - вектор, в якому потрібно замінити значення;

2) shape_data$ADM1_UA == "Автономна Республіка Крим" - значення, яке потрібно замінити;

3) "АР Крим" - значення, на яке потрібно замінити.

Виконавши необхідні підготовчі дії, об'єднаємо статистичний та географічний датафрейми за полями з назвами адміністративно-територіальних одиниць. Використаємо для цього пайп-оператор %>% та функцію left_join() (рис. 30.13, рядок 15).

```
14  # Об'єднання географічної та статистичної баз даних за назвою регіону
15  shape_data<-shape_data %>% left_join(data, by = c( "ADM1_UA"="Region" ))
```

Рисунок 30.13. Скрипт обєднання датафреймів

Пайп-оператор %>% використовується для з'єднання кількох функцій в одну послідовність.

Функція left_join() використовується для об'єднання двох наборів даних, використовуючи значення в першому наборі даних як ключі.

> *Ключі наборів даних - це значення, які використовуються для об'єднання двох наборів даних. Ключі повинні бути унікальними в кожному наборі даних, щоб забезпечити правильне об'єднання.*

Функція повертає новий набір даних, який містить всі записи з першого набору даних, а також записи з другого набору даних, у яких відповідні ключі збігаються.

В нашому випадку, виконання даної частини скрипту приведе до формування датафрейму, де кожній адміністративно-територіальній одиниці буде відповідати два записи (2021 та 2022 рік).

Наступним кроком, необхідно сформувати окремі набори даних для шарів майбутньої картограми. Виходячи з умов кейсу такими шарами будуть дані за 2021 рік та дані за 2022 рік (рис. 30.14).

```
17  # Отримання даних для шарів картограми (по роках)
18  shape_data_2022 <- shape_data %>% filter(Year == 2022)
19  shape_data_2021 <- shape_data %>% filter(Year == 2021)
```

Рисунок 30.14. Скрипт формування даних для шарів картограми

Нарешті для побудови картограми знадобиться кольорова шкала. Побудуємо її за допомогою функції colorBin() та призначимо для змінної pal_d (рядки 23 та 24, рис. 30.15).

```
21  # Функція для визначення кольорів регіональних полігонів
22  # залежно від кількості облікованих проваджень
23  pal_d<-colorBin(palette =  c('#006837','#a6d96a','#ffffbf','#fdae61','#a50026'),
24                  domain = shape_data$ACC, bins = 5)
```

Рисунок 30.15. Скрипт для визначення кольорів за регіонами

Функція colorBin() використовується з метою створення шкали кольорів для відображення даних на карті. Вона приймає три аргументи: 1) palette - палітра кольорів, яка буде використовуватися для відображення даних; 2) domain - діапазон даних, які потрібно відобразити; 3) bins - кількість відтінків кольору, які потрібно використовувати. У випадку нашого кейсу палітру складають кольори, що традиційно використовуються для візуалізації рельєфу на фізичних мапах (рядок 23, рис. 15), діапазон даних – всі можливі значення кількості облікованих проваджень за ознаками крадіжки у 2021 або 2022 році, кількість відтінків дорівнює п'яти.

Побудова картограми. Побудова картограми відбувається шляхом призначення певній змінній, в нашому випадку map, результату виконання функції leaflet() (рис. 30.16):

```
26  #Побудова картограми
27  map<-leaflet()%>%setMaxBounds(20,45,41,53)%>%addProviderTiles("Esri.WorldGrayCanvas")%>%
28    addPolygons(data=shape_data_2021,group = "2021",
29                weight=1,fillOpacity = 0.6,
30                color = pal_d (shape_data_2021$ACC),
31                popup = ~paste0("<b>", ADM1_UA, "</b>",
32                    "<br/>","Кількість облікованих проваджень у 2021 році:", ACC),
33                highlight = highlightOptions(weight = 3, color = "white"))%>%
34    addPolygons(data=shape_data_2022,group = "2022",
35                weight=1,fillOpacity = 0.6,
36                color = pal_d (shape_data_2022$ACC),
37                popup = ~paste0("<b>", ADM1_UA, "</b>",
38                    "<br/>","Кількість облікованих проваджень у 2022 році: ", ACC),
39                highlight = highlightOptions(weight = 3, color = "white"))%>%
40    addLayersControl(baseGroups = c("2021","2022"), )%>%
41    addControl(html = "Географічний розподіл проваджень,
42  облікованих у 2021 та 2022 роках за ознаками крадіжки",position = "bottomright")
```

Рисунок 30.16. Скрипт побудови картограми

Прокоментуємо дану частину скрипту. Команди у рядку 27, map<-leaflet() %>%setMaxBounds(20,45, 41,53)%>%addProviderTiles("Esri.WorldGrayCanvas"), ініціюють створення віджету з фізичною мапою, обмежують поле відображення. Зазначимо, що в даному випадку для фонової мапи ми використали представлений у вільному доступі набір даних компанії Esri. Команди у рядках 28-33 забезпечують створення шару картограми з даними 2021 року. Команди у рядках 34-39 забезпечують створення шару картограми з даними 2022 року. Команда addLayersControl (рядок 40) забезпечує включення до віджету елемен-

ту для перемикання шарів. Команда addControl (рядки 41 та 42) забезпечує додавання до віджету текстової анотації.

Створення річних шарів забезпечується командою addPolygons, яка додає до віджету полігони областей, міст Києва та Севастополя. Охарактеризуємо параметри даної функції, використані для розв'язання кейсу:

data – *набір даних для шару полігонів;*
group – *назва шару, яка буде використовуватися у меню керування шарами, які відображує віджет;*
weight – *товщина межі полігону;*
fillOpacity – *прозорість заповнення полігону;*
color – *колір полігону, що залежить від раніше визначеної функції pal_d;*
popup – *зміст повідомлення, яке буде з'являтися при виборі полігону;*
highlight – *реакція полігону при появі вказівника над ним (в нашому випадку, зміна товщини та кольору меж полігону).*

Виведення та збереження картограми. Команда map (рис. 30.17, рядок 46) забезпечує виведення отриманої картограми у вікно Viewer використовуваного нами програмного середовища.

```
45  # Виведення картограми у вікно Viewer
46  map
47
48  # Збереження картограми у файл *.html
49  saveWidget (map, "map.html")
```

Рисунок 30.17. Скрипт виведення картограми

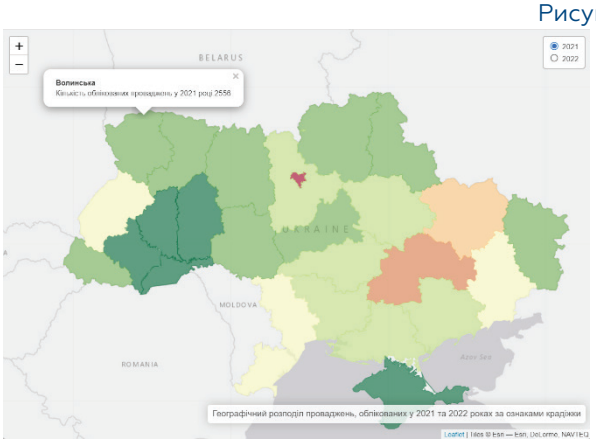


Рисунок 30.18. Картограмма за кількістю злочинів у регіонах

Використання функції saveWidget () приведе до створення файлу map.html, в якому буде збережено створений віджет.

Отримана картограма (рис. 33.18) відповідає завданням практичного кейсу:

- *візуалізує необхідні дані, кримінальних проваджень, облікованих у 2021 та 2022 році за ознаками крадіжки;*
- *є інтерактивною, вибір полігону приводить до появи інформативного вікна, а при появі вказівника над полігоном виділяються його межі;*
- *має два шари, дані 2021 року та дані 2022 року, їх перемикання забезпечується елементом у правому верхньому куті;*
- *зберігається в окремому файлі *.html.*

Повний скрипт для розв'язання цієї частини кейсу представлено у файлі map.R репозиторію R_case.

Уданому практичному кейсі було продемонстровано основні можливості R щодо збирання даних, здійснення операцій з ними та візуалізації. Далі наводиться описання реалізованого нами проєкту інтерактивного довідника даних офіційної статистики щодо протидії злочинності в Україні.

РЕАЛІЗОВАНИЙ В R ПРОЄКТ З АНАЛІЗУ ДАНИХ ОФІЦІЙНОЇ СТАТИСТИКИ ЩОДО ПРОТИДІЇ ЗЛОЧИННОСТІ В УКРАЇНІ

Проблема. В Україні недостатньо інструментів аналізу публічних даних щодо протидії злочинності. Це унеможливлює проведення якісних наукових досліджень, які б ґрунтувалися на даних, обмежує можливості оцінки ефективності правоохоронної діяльності, призводить до незбалансованих змін кримінального законодавства, ускладнює моніторинг реформи кримінальної юстиції.

Базові показники кримінально-правового регулювання представлено у вигляді періодичних звітів у форматі електронних таблиць доступних для завантаження з сайтів ОГП та ДСА України. Такий формат даних істотно ускладнює роботу з ними. Отримання знань щодо ефективності протидії злочинності на підставі аналізу відкритих статистичних даних обмежено необхідністю проведення складних технічних операцій.

Відповідно, результати роботи правоохоронних та судових органів не є прозорими, механізм демократичного нагляду за їх діяльністю не є достатньо ефективним.

Запропоноване розв'язання. Автором [5] розроблено та представлено у відкритому доступі [12] веб застосунок для аналізу значної частини цього масиву інформації.

Методологію розробки застосунку характеризують юридичний, алгоритмічний та технічний складники.

Юридичний полягає в тому, що вхідні дані ми розглядаємо з усталених і найбільш поширених позицій правової науки. Зокрема, це стосується змісту використовуваних у дослідженні понять «кримінальне правопорушення», «обліковане правопорушення», «вирок, що набрав чинності» тощо. Розгляд процесу протидії злочинності зумовлений змістом аналізованих статистичних звітів.

У загальних рисах процес протидії злочинності, представлений у статистичних звітах, полягає у наступному:

1) певні події правоохоронні органи обліковують як такі, що потребують дослідження в межах кримінальних проваджень;

2) у результаті досудового розслідування таких подій може бути прийнято рішення про скерування матеріалів провадження до суду;

3) у такому разі можливі чотири варіанти: скерування матеріалів з обвинувальним актом, скерування клопотання про звільнення від кримінальної відповідальності, скерування клопотання про застосування примусових заходів медичного характеру, скерування клопотання про застосування примусових заходів виховного характеру;

4) розгляд матеріалів провадження в суді закінчується набранням чинності певним судовим рішенням;

5) такі рішення також можуть бути чотирьох різновидів: про засудження особи, про виправдання особи, про застосування примусових заходів медичного характеру та про закриття справи;

6) якщо особа визнається винною, реалізація кримінальної відповідальності може відбуватися в репресивній (призначення покарання) або ліберальній (звільнення від покарання) формах.

Представлені у відкритому доступі та використані як вхідні дані річні звіти Офісу Генерального Прокурора України та Державної судової адміністрації України є результатом покладених на ці органи обов'язків, передбачених відповідними нормативними документами [13;14].

Алгоритмічний складник стосується особливостей проведення відтворюваного дослідження (reproducible research). Збір даних відбувається в спосіб завантаження звітів, представлених на офіційних інтернет-представництвах Офісу Генерального прокурора України та Державної судової адміністрації України. Посилання на звіти додано до відповідних програмних скриптів. Виконання скриптів дає змогу отримати локальні копії вхідних даних. Трансформація даних у цьому дослідженні полягала в перетворенні звітів на дані, придатні для автоматизованого опрацювання («чисті» дані). На підставі аналізу особливостей структури вхідних звітів було розроблено скрипти очищення даних. Виконання цих скриптів дало змогу отримати файли, що містять тільки показники кримінально-правового регулювання, властиві певним статтям Особливої частини КК. У цих файлах відсутні елементи, які утруднюють автоматизовану обробку (розмітка таблиць, підсумкові рядки, заголовки тощо). Скрипти автоматизованої обробки створюють з отриманих на попередньому етапі «чистих» даних добірки та узагальнення для дальших візуалізацій. Візуалізація здійснюється знову ж таки через виконання скриптів, що використовують добірки, отримані на попередньому етапі, і стандартні бібліотеки графічного представлення даних.

Технічний складник полягає в характеристиці застосованого програмного забезпечення. Для виконання завдань дослідження використовувалася мова програмування R середа розробки програмного забезпечення з відкритим вихідним кодом RSudio. Розробку оболонки веб-застосунку здійснено з використанням Shiny R - програмного середовища для створення інтерактивних програмних продуктів з графічним інтерфейсом на основі мови програмування R. Для розробки застосунку використано такі бібліотеки (libraries) R:

Shiny [15],
readxl [16],
readr [17],
DT [18],
xlsx [19],
tidyverse [7],
textreadr [20],
stringr[21],
leaflet [22].

В онлайн-додатках представлено вихідні дані, дані, придатні до автоматизованої обробки, програмні коди для отримання первинних даних, їх обробки й візуалізації [23]. Всі використані програмні продукти та дані представлено у вільному доступі, що є додатковою гарантією можливості відтворення здійсненого дослідження

Основні характеристики веб-застосунку «Протидія злочинності в Україні: інфографіка».

Довідник представлено у вигляді веб-застосунку, який інтегрує та дає можливість аналізувати дані, що містяться у звітах Офісу Генерального прокурора України та Державної судової адміністрації:

- *період спостережень охоплює десять років (2013-2022);*
- *більше ніж 100 параметрів аналізу застосування кримінального законодавства;*
- *набір даних, який налічує більше 10 мільйонів показників функціонування національної системи кримінальної юстиції;*
- *режим створення власних візуалізацій та наборів даних, можливість комбінувати параметри, визначати період спостережень, рівень узагальнення, та необхідність обрахунку відносних значень;*
- *режим побудови фонових картограм на основі регіональних даних.*

ВИКОРИСТАНІ ДЖЕРЕЛА

1. R Core Team (2022). R: A language and environment for statistical computing. R. Foundation for Statistical Computing, Vienna, Austria. Retrieved from https://www.R-project.org/
2. Data Analysis with R Programming. Google Data Analytics professional certification program. Retrieved from https://www.coursera.org/learn/data-analysis-r
3. Карчевський М.В. Аналіз та операції з великими даними в середовищі R (практичний кейс). Репозиторій GitHub. URL: https://github.com/Nickolay78/R_case
4. Karchevskyi M. R_case - project. Part of practical case «Big data analysis and operations in the R environment». URL: https://posit.cloud/content/6972036
5. Карчевський М.В. Протидія злочинності в Україні у форматі DATA SCIENCE. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка.* 2022. № 2(98). С. 202-227.
6. Протидія злочинності в України: інфографіка. Репозиторій. URL: field_n.xlsx
7. Wickham et al. (2019). Welcome to the tidyverse. *Journal of Open Source Software*, 4(43), 1686.
8. Cheng, J., Schloerke, B., Karambelkar, B. & Xie, Y. (2023). _leaflet: Create Interactive Web Maps with the JavaScript 'Leaflet' Library. R package version 2.2.0. Retrieved from https://CRAN.R-project.org/package=leaflet
9. Pebesma, E. & Bivand, R. (2023). Spatial Data Science: With Applications in R. Chapman and Hall/CRC. https://doi.org/10.1201/9780429459016; Pebesma, E., 2018. Simple Features for R: Standardized Support for Spatial Vector Data. The R Journal 10 (1), 439-446. Retrieved from https://doi.org/10.32614/RJ-2018-009
10. Vaidyanathan R., Xie Y., Allaire J., Cheng J., Sievert C. & Russell., K. (2023). _htmlwidgets: HTML Widgets for R. R package version 1.6.2. Retrieved from https://CRAN.R-project.org/package=htmlwidgets
11. Ukraine - Subnational Administrative Boundaries. - The Humanitarian Data Exchange. Retrieved from https://data.humdata.org/dataset/cod-ab-ukr
12. Карчевський М. Протидія злочинності в Україні: інфорграфіка: інтерактивний довідник. Версія 3.0. URL : https://karchevskiy.com/i-dovidnyk/
13. Про затвердження річних форм звітів щодо здійснення правосуддя місцевими та апеляційними судами. Наказ Державної судової адміністрації України від 23.06.2018 № 325.
14. Про затвердження форм єдиної звітності про стан кримінальної протиправності. Наказ Офіса Генерального Прокурора України від 30.06.2020 № 299.
15. Winston Chang, Joe Cheng, JJ. Allaire, Carson Sievert, Barret Schloerke, Yihui Xie, Jeff Allen, Jonathan McPherson, Alan Dipert & Barbara Borges (2021). Shiny: Web Application Framework for R. R package version 1.7.1. https://CRAN.R-project.org/package=shiny
16. Hadley, Wickham & Jennifer, Bryan (2022). Readxl: Read Excel Files. R package version 1.4.0. Retrieved from https://CRAN.R-project.org/package=readxl
17. Hadley, Wickham, Jim, Hester & Jennifer, Bryan (2022). Readr: Read Rectangular Text Data. R package version 2.1.2. Retrieved from https://CRAN.R-project.org/package=readr
18. Yihui, Xie, Joe, Cheng & Xianying, Tan (2022). DT: A Wrapper of the JavaScript Library 'DataTables'. R package version 0.22. Retrieved from https://CRAN.R-project.org/package=DT
19. Adrian, Dragulescu & Cole, Arendt (2020). Xlsx: Read, Write, Format Excel 2007 and Excel 97/2000/XP/2003 Files. R package version 0.6.5. Retrieved from https://CRAN.R-project.org/package=xlsx
20. Rinker, T. W. (2021). Textreadr: Read Text Documents into R version 1.2.0. Buffalo, New York. Retrieved from https://github.com/trinker/textreadr
21. Hadley, Wickham (2019). Stringr: Simple, Consistent Wrappers for Common String Operations. R package version 1.4.0. Retrieved from https://CRAN.R-project.org/package=stringr
22. Cheng, J., Schloerke, B., Karambelkar, B. & Xie, Y. (2023). _leaflet: Create Interactive Web Maps with the JavaScript 'Leaflet' Library. R package version 2.2.0. Retrieved from https://CRAN.R-project.org/package=leaflet .
23. Input data, scripts for collecting, cleaning, processing and building visualizations for web-application by M. Karchvskyi "Interactive reference book "Combating Crime in Ukraine" (2013-2022). Retrieved from https://github.com/Nickolay78/Ukraine_2013-2022

DOI: https://doi.org/10.36486/978-966-2310-66-5-31

...розкриття злочинів – це не стільки наука, скільки мистецтво

Ніро Вульф

РОЗДІЛ 31

Фінансові розслідування для ефективного розслідування складних кримінальних правопорушень

Ганна Горбенко

Вчинення складних кримінальних правопорушень, можуть різко зростати і загострювати проблеми, які постають перед урядами під час реагування на кризу та відновлення, у тому числі під час збройних конфліктів. Кризові ситуації часто призводять до швидкої мобілізації ресурсів, послаблення механізмів нагляду та запровадження надзвичайних заходів, що підвищують ризики корупції, відмивання доходів, отриманих злочинним шляхом, інших економічних злочинів. Це не лише підриває ефективність заходів реагування, але й підриває довіру громадськості до інституцій, що потенційно може затягнути кризу та зменшити темпи відновлення. Як наслідок, рішучі заходи, в тому числі посилення фінансових розслідувань, є важливими інструментами для ефективного реагування.

Фінансові розслідування відіграють ключову роль у боротьбі з кримінальною фінансовою злочинністю. Вони дозволяють розкривати і розслідувати різні види злочинів, які пов'язані з грошима і фінансовими операціями, такі як відмивання грошей, корупція, фінансування тероризму, шахрайство, податкові шахрайства і багато інших.

Фінансові розслідування надають можливість:

- ***розкривати злочини:*** *фінансові розслідування допомагають виявляти і документувати* ***факти злочинів****, що пов'язані з фінансовими операціями. Вони дозволяють знайти як правопорушників, так і співучасників, а також виявляти мережі фінансових злочинів.*
- ***відслідковувати відмивання грошей:*** *фінансові розслідування допомагають виявляти і відслідковувати* ***грошові потоки****, які використовуються для приховування незаконно отриманих коштів, що є необхідним етапом для боротьби з відмиванням грошей і конфіскацією незаконно нажитого майна.*
- ***виявляти корупцію:*** *фінансові розслідування дозволяють виявляти* ***корупційні схеми****, які зазвичай включають у себе розкрадання державних коштів або хабарництво, що може допомогти припинити корупційну діяльність і притягнути винних до відповідальності.*
- ***боротися з фінансуванням тероризму:*** *фінансові розслідування є ключовим інструментом для виявлення та переслідування фінансування* ***терористичних організацій****.*
- ***попереджати фінансові злочини:*** *фінансові розслідування можуть слугувати засобом запобігання* ***фінансовим злочинам****. Аналіз фінансових даних і виявлення нетипових операцій можуть допомогти вчасно виявити можливі порушення.*
- ***використовувати інструменти:*** *у фінансових розслідуваннях використовуються* ***різні інструменти****, такі як банківські записи, фінансові звіти, електронні платежі, біткоіни та інші криптовалюти. Різні програмні інструменти для аналізу даних дозволяють аналізувати та відстежувати фінансові операції.*
- ***співпрацювати з міжнародними партнерами:*** *фінансові розслідування часто потребують* ***міжнародного співробітництва****, оскільки злочинці можуть використовувати міжнародні фінансові системи для викривлення слідів. Міжнародні організації і міжнародні угоди дозволяють обмінюватися інформацією і спільно розслідувати фінансові злочини.*

Усі ці аспекти демонструють важливість фінансових розслідувань у боротьбі з сучасною фінансовою злочинністю. Вони допомагають не лише розкривати злочини, але і запобігати їх вчиненню, забезпечуючи більшу безпеку і справедливість у суспільстві.

ОСНОВИ ФІНАНСОВИХ РОЗСЛІДУВАНЬ.

Фінансові розслідування в кримінальних провадженнях мають кілька фундаментальних концепцій і елементів, які відіграють важливу роль у проведенні ефективних кримінальних розслідувань, зокрема в боротьбі з складними економічними злочинами/відмиванням доходів, одержаних злочинним шляхом/корупцією.

Основні концепції включають в себе:

- ✓ ***аналіз фінансових даних**, що передбачає аналіз фінансових документів, банківських виписок, податкових звітів, бухгалтерських записів та інших фінансових даних для виявлення нетипових операцій, відмивання грошей та інших ознак злочинів;*
- ✓ ***виявлення патернів** чи шаблонів, що можуть включати виявлення незаконних платежів, надмірних розходів, невідповідності між доходами та видатками, чи інші аномалії у фінансових документах;*
- ✓ ***відслідковування грошових потоків** і фінансових транзакцій, що допомагає виявити переміщення і перетворення грошей у інші активи. Розуміння платіжних систем і фінансових інструментів, таких як SWIFT (Society for Worldwide Interbank Financial Telecommunication), дозволяє слідчим відстежувати міжнародні фінансові потоки та перекази грошей. SWIFT є важливим інструментом для виявлення фінансових злочинів, і слідчі можуть отримувати доступ до інформації про міжнародні банківські транзакції через запити до банків.*
- ✓ ***електронні сліди**: з використанням електронних засобів сплати і банківських транзакцій дедалі більше фінансових даних стають електронними;*
- ✓ ***об'єднання інформації з різних джерел**, таких як банки, компанії, податкові служби та інші джерела, для створення повної картини фінансових операцій;*
- ✓ ***аналітичні інструменти** та програми для обробки великих обсягів даних можуть значно полегшити аналіз фінансової інформації та виявлення незаконних фінансових потоків. Вони допомагають в ефективному розгортанні слідчого процесу.*

Застосування цих концепцій і елементів протягом усього слідчого циклу допомагає не лише виявляти складні економічні злочини/відмивання доходів, одержаних злочинним шляхом/корупцію, але і забезпечувати належну доказову базу для притягнення винних до відповідальності.

> *Важливо пам'ятати, що фінансові розслідування вимагають великої експертизи, ресурсів та спеціалізованих знань, але є необхідним інструментом у боротьбі з складними економічними злочинами/відмиванням доходів, одержаних злочинним шляхом/корупцією.*

ВІДСТЕЖЕННЯ КОРУПЦІЙНИХ ДОХОДІВ.

Відстеження походження незаконних коштів і розкриття їхнього шляху використання є критично важливим завданням у боротьбі з корупцією та іншими фінансовими злочинами. Ось деякі ключові причини, чому важливо відстежувати походження коштів:

- ➢ ***допомагає ідентифікувати** осіб, які вчиняли корупційні дії або інші фінансові злочини. Це дає можливість притягти їх до відповідальності та покарати за скоєні злочини.*
- ➢ ***дозволяє знайти активи**, які було придбані за кошти, отримані від корупційних дій. Це дає можливість повернути вкрадені кошти на користь суспільства або потерпілих сторін.*
- ➢ ***допомагає запобігти** їхній легалізації через різноманітні механізми, такі як нерухомість, бізнеси та інші інвестиції.*
- ➢ ***успішні розслідування** корупційних справ підвищують довіру громадськості до правоохоронних органів і демонструють ефективність боротьби з корупцією,*

але одночасно можуть бути потенційні ускладнення, з якими можуть зіткнутися слідчі через використання поширених методів приховування незаконних активів:

- ○ *відкриття рахунків в іноземних банках або використовувати псевдоніми для приховування своїх коштів.*
- ○ *інвестування незаконно нажиті кошти в легальні бізнеси та активи, роблячи їх складними до відслідковування.*
- ○ *використання криптовалют може ускладнити виявлення незаконних фінансових потоків, оскільки вони можуть бути анонімними і не підлягати контролю.*
- ○ *використання осіб, які не мають кримінальної історії, для здійснення транзакцій та приховування активів.*

ВІДМИВАННЯ ГРОШЕЙ ТА ПОВ'ЯЗАНІ З НИМ ЗЛОЧИНИ.

Розглянувши природу відстеження коштів, розглянемо загальні методи, що використовуються для приховування активів, отриманих незаконним шляхом, що є невід'ємною частиною процесу відмивання грошей. Ось деякі загальні методи, які злочинці можуть використовувати для приховування своїх незаконних активів:

- ***вкладення в нерухомість**, наприклад квартири, будинки або комерційні об'єкти. Це може виглядати як легальна інвестиція, і активи можуть бути використані для житла або оренди, при цьому приховуючи їх походження.*
- ***вкладення в бізнес**, наприклад створення фіктивних бізнесів або інвестування в існуючі компанії. Ця діяльність може включати придбання акцій, запуск нових проектів або збільшення обороту підприємства.*
- ***використання іноземних банківських рахунків**, в тому числі за кордоном, де законодавство про фінансову конфіденційність більш лояльне. Це дозволяє приховувати гроші та уникати спостереження.*
- ***використання фіктивних імен** та псевдонімів, номінальних власників для реєстрації активів та транзакцій, ускладнюючи відстеження власника.*
- ***криптовалюти** надають можливість анонімних фінансових транзакцій і можуть бути використані для приховування незаконно нажитих активів.*
- ***переведення активів** до офшорних компаній.*

Зв'язок між корупційними злочинами і відмиванням грошей полягає в тому, що перші нерідко призводять до других. Корупційні злочини, такі як хабарі, розкрадання бюджетних коштів чи інші форми зловживання владою, можуть призвести до незаконних фінансових надходжень. Після вчинення корупційного злочину особа зазвичай намагається «відмити» отримані незаконні активи, щоб приховати їхнє походження та надати їм легальний статус. Звідси виникає важливість розроблення загальних методів виявлення та запобігання відмиванню грошей у контексті корупційних злочинів. Щоб приховати ці незаконні активи і зробити їх легальними, злочинці використовують вище згадані розповсюджені методи відмивання грошей.

> *Правоохоронцям і слідчим слід приділяти особливу увагу виявленню незаконних активів та розкриттю схем відмивання грошей, оскільки це може призвести до розкриття корупційних дій і притягнення злочинців до відповідальності.*

ПІДГОТОВКА ПЛАНУ ФІНАНСОВИХ РОЗСЛІДУВАНЬ.

Розробка плану фінансових розслідувань включає в себе кілька важливих кроків і аспектів, які допомагають зіставити наявні фінансові докази, збирати нові дані та визначати потрібні докази для подальшого просування справи. Ось **загальні підходи розроблення такого плану**:

(a) зіставлення наявних фінансових доказів:

1. *оцінка наявних доказів*: спочатку слід провести оцінку всіх наявних фінансових доказів, включаючи банківські виписки, податкові декларації, бухгалтерські записи, контракти та інші фінансові документи.
2. *визначення ключових пунктів:* виокреміть ключові факти та пункти, які можуть вказувати на корупційні або незаконні дії. Це включає в себе незвичайні транзакції, великі суми грошей, невідповідності у фінансових записах тощо.

(b) збір фінансових доказів:

1. *додаткові документи:* з'ясуйте, які фінансові документи та інформація ще потрібні, і розробіть план для їх збору. Це може включати в себе запити до банків, аудиторських фірм, податкових служб, а також свідчень і показань свідків.
2. *висновок:* зверніть увагу на зберігання даних в електронному вигляді.
3. *аналіз банківських операцій:* проведіть аналіз банківських виписок та транзакцій, щоб виявити незвичайні операції або перекази.

(c) визначення доказів, які ще потрібні для продовження розслідування:

1. *ідентифікація «білих плям»:* з'ясуйте, чи є інші особи або компанії, які можуть бути причетні до корупційних дій, і спрямовуйте зусилля на їх виявлення.

2. *використання спеціалізованих служб:* ви можете співпрацювати з фахівцями у сфері фінансових розслідувань, аудиторів, бухгалтерів та іншими спеціалістами для збору та аналізу додаткових доказів.

(d) ресурси та пріоритети:

1. *визначення ресурсів:* оцініть, які ресурси (людські, технічні, фінансові) потрібні для проведення фінансового розслідування та забезпечення їх наявності.
2. *встановлення пріоритетів:* визначте порядок дій і пріоритети для збору та аналізу доказів. Подумайте про терміни та стратегії для кожного етапу розслідування.
3. *співпраця:* співпрацюйте з іншими правоохоронними органами, а також з міжнародними організаціями та іншими стейкхолдерами, які можуть надати додаткову підтримку та ресурси.

> *Важливо пам'ятати, що фінансове розслідування може бути складним, а часом - ресурсоємким процесом. Ефективне планування і систематичний підхід є ключовими для успішного проведення фінансового розслідування в контексті складних економічних злочинів/відмивання доходів, одержаних злочинним шляхом/корупційних злочинів.*

ЗВІТ ПРО ПЛАН ФІНАНСОВИХ РОЗСЛІДУВАНЬ.

Звіт про план фінансових розслідувань є важливим інструментом для узгодження та планування подальших кроків у розслідуванні фінансових злочинів. Цей звіт повинен містити докладний огляд плану розслідування та включати різні аспекти, такі як опис наявних фінансових доказів, стратегію збору додаткових доказів, оцінку необхідних ресурсів та пріоритети.

Ось **загальна структура звіту** про план фінансових розслідувань:

1. Заголовок та вступ:
   - *Вкажіть назву звіту та вступний коментар, що відображає мету та контекст розробки плану.*
2. Огляд наявних фінансових доказів:
   - *Опишіть наявні фінансові докази, які були зібрані або ідентифіковані до моменту розробки плану розслідування.*
   - *Зазначте, яку інформація вони містять та як вони стосуються підозрюваних у фінансових злочинах.*
3. Стратегія збору додаткових фінансових доказів:
   - *Опишіть стратегію та методи, які будуть використовуватися для збору додаткових фінансових доказів.*
   - *Визначте конкретні джерела інформації, які будуть перевірені, і методи, які будуть використані для збору цих доказів.*
4. Визначення докази, які ще потрібні для подальшого розслідування:
   - *Визначте, які конкретні докази або інформація ще потрібні для встановлення вини або невинності підозрюваних.*
   - *Опишіть, які відомості або докази важливі для вирішення справи.*
5. Оцінка ресурсів та пріоритетів:
   - *Визначте, які ресурси, включаючи людські, фінансові та технічні, будуть необхідні для виконання плану розслідування.*
   - *Встановіть пріоритети для кожного етапу розслідування та визначте, які кроки мають бути виконані першими.*
6. Додаткові матеріали справи:
   - *Включіть додаткові матеріали, які можуть бути важливими для розслідування, такі як копії документів, звітів, свідчень тощо.*
7. Заключні висновки та рекомендації:
   - *Завершіть звіт заключними висновками та рекомендаціями щодо подальших кроків у розслідуванні фінансових злочинів.*

> *Звіт про план фінансових розслідувань має бути чітким, логічним та докладним, щоб всі учасники розслідування могли розуміти його зміст та спрямовувати свої зусилля відповідно до запропонованого плану.*

Після розгляду звіту можуть бути внесені корективи та покращення в залежності від обставин та нових доказів, що з'являться в процесі розслідування.

ОСНОВИ СУДОВОЇ БУХГАЛТЕРІЇ.

Базові методи судово-бухгалтерської експертизи є незамінними для слідчих та аналітиків для виявлення сумнівних транзакцій. Досконале розуміння цих методів може прискорити процес окреслення повної картини корупційних потоків коштів.

Ось **деякі з базових методів** судово-бухгалтерської експертизи:

Аналіз бухгалтерських звітів:

Огляд бухгалтерських звітів, таких як баланс, звіт про прибутки та звіт про готівкові розрахунки, для виявлення аномалій та неправомірних транзакцій.

Порівняльний аналіз:

Порівняння фінансових даних різних періодів для виявлення змін та незвичайних коливань.

Аналіз фінансових відомостей:

Вивчення фінансових відомостей, включаючи банківські виписки, чеки та квитанції, для виявлення аномалій та незвичайних транзакцій.

Аналіз банківських операцій:

Вивчення банківських операцій, включаючи грошові перекази та платіжні доручення, для виявлення незаконних фінансових потоків.

Відстеження активів:

Дослідження активів та власності підозрюваних осіб для виявлення незаконних активів та їхнього походження.

Перевірка фінансових документів:

Перевірка правдивості та достовірності фінансових документів, які можуть бути використані для виявлення шахрайства чи фіктивних транзакцій.

Аналіз податкових декларацій:

Огляд податкових декларацій для виявлення розбіжностей між податковими зобов'язаннями та фінансовими даними.

Експертиза електронних даних:

Аналіз електронних фінансових даних, включаючи електронні звіти та електронні банківські виписки.

> *Зрозуміння та використання цих методів допомагає слідчим та аналітикам виявляти та розкривати корупційні дії, а також узгоджувати фінансову інформацію для розслідування.*

Додатковою перевагою є можливість використання спеціалізованих програм та інструментів для більш точного та ефективного аналізу фінансових доказів.

СКЛАДАННЯ СХЕМ ФІНАНСОВИХ ДОКАЗІВ.

Складання схем і діаграм є важливою частиною аналізу фінансових доказів у розслідуванні корупції та інших фінансових злочинів. Схеми та діаграми можуть візуалізувати складні дані та патерни, що допомагають зрозуміти зв'язки і спростити прийняття рішень. Ось **загальний огляд процесу** аналізу фінансових доказів та побудови схем:

1. Збір та обробка даних:
    - *Почніть зі збору всіх наявних фінансових доказів, таких як бухгалтерські звіти, банківські виписки, інвестиційні рахунки та інше.*
    - *Очистіть та підготуйте дані для аналізу, видаливши зайві або недійсні записи.*
2. Визначення мети графіків:
    - *Визначте, якою інформацією ви хочете поділитися або який аспект аналізу ви хочете візуалізувати.*
    - *Мета графіків може бути виявленням тенденцій, аномалій, порівнянням даних тощо.*

3. Вибір типу графіків:
   - *Виберіть відповідний тип графіків або діаграм (лінійні, кругові, стовпчасті тощо), який найкраще відобразить вашу інформацію.*
4. Побудова графіків:
   - *Використовуйте спеціалізовані програми для створення графіків, такі як Microsoft Excel, Python, I2 тощо.*
   - *Додайте дані до графіків та налаштуйте їх для досягнення бажаного вигляду та інформативності.*
5. Аналіз графіків:
   - *Аналізуйте побудовані графіки та діаграми для виявлення патернів, аномалій чи інших важливих висновків.*
   - *Визначте, які інсайти можна здобути з графіків та як вони вплинуть на подальші дії в розслідуванні.*
6. Подальші кроки:
   - *На основі аналізу графіків і діаграм визначте, які додаткові матеріали або докази потрібні для поглибленого розслідування.*
   - *Розробіть план подальших кроків, включаючи видачу запитів на документи, опитування свідків та інші дії.*

> *Після побудови схем та аналізу їх результатів, важливо працювати над подальшими кроками розслідування та розглядати можливості для покращення аналізу фінансових доказів.*

У деяких випадках, робота в малих групах або з іншими експертами може допомогти отримати додаткові інсайти та розробити стратегію розслідування.

ОПИТУВАННЯ СВІДКІВ ТА ПІДОЗРЮВАНИХ У ФІНАНСОВИХ ЗЛОЧИНАХ.

Окрім документальних доказів, для слідчих не менш важливо отримати чітке визнання вини від злочинців, особливо щодо того, як вони здійснювали свої транзакції. Розглянемо методи допиту у справах про фінансові злочини та як максимально ефективно використовувати допит як ключову можливість для збору доказів.

Нижче наводимо деякі **методи і поради щодо допиту в справах про фінансові злочини**:

- ✓ *підготовка до допиту.* Перед допитом ретельно вивчіть всі наявні докази та інформацію про справу. Розробіть план допиту, включаючи запити про конкретні факти, транзакції та інші деталі, які вас цікавлять.
- ✓ *встановлення контакту та побудова довіри.* Спробуйте встановити позитивний контакт та побудувати довіру з особою, яку ви допитуєте. Слухайте уважно та поважайте позицію свідка чи підозрюваного.
- ✓ *використання відкритих питань.* Використовуйте відкриті питання для стимулювання докладних розповідей та отримання деталей.
- ✓ *запити про конкретні факти.* Поставте запити щодо конкретних фактів, транзакцій чи подій, щоб отримати докладну інформацію.
- ✓ *визнання вини.* В питаннях стосовно вини формулюйте їх так, щоб вони були конкретними і не залишали місця для ухилення. Спрямовуйте запити на визнання фактів чи дій, які вказують на вину.
- ✓ *врахування правових обмежень.* Пам'ятайте про правові обмеження, такі як право на невідомість, інформаційну привілею та інші права свідків і підозрюваних.
- ✓ *документування.* Детально документуйте відповіді та висновки з допиту. Це допоможе в подальшому використовувати інформацію в судовому процесі.
- ✓ *відсутність тиску.* Уникайте тиску на свідків чи підозрюваних, оскільки це може призвести до невірних зізнань.
- ✓ *співпраця зі спеціалістами.* У деяких випадках співпраця зі спеціалістами, такими як психологи або кримінальні профілісти, може допомогти покращити результати допиту.
- ✓ *співпраця з іншими службами.* Розгляньте можливість співпраці з іншими службами, такими як прокуратура чи поліція, для забезпечення високої ефективності розслідування.

- ✓ *ефективний допит* може бути ключовим для отримання важливих відомостей та визнання вини у справі про фінансові злочини. Правильна підготовка та професійний підхід допомагають слідчим здійснити дієвий аналіз фінансових доказів і отримати важливу інформацію для розслідування.

АНАЛІЗ ДОКАЗІВ ТА ПЕРЕГЛЯД ПЛАНУ.

Важливим етапом ефективного проведення фінансового розслідування є перегляд Плану фінансового розслідування, включно з відповідями на такі питання:

(a) Структура злочинної організації.
(b) Відображення фінансових потоків.
(c) Які цілі розслідування?
(d) Які ще докази потрібні для притягнення до відповідальності?

Схема доказів та перегляд плану фінансового розслідування може виглядати наступним чином:

План фінансового розслідування:

1. Структура злочинної організації:
   - *Основні фігури та учасники злочинної організації.*
   - *Ролі та обов'язки кожного члена організації.*
   - *Зв'язки та ієрархія в організації.*
2. Відображення фінансових потоків:
   - *Аналіз бухгалтерських звітів, банківських виписок та інших фінансових документів.*
   - *Виявлення патернів та потоків грошей між особами та організаціями.*
   - *Встановлення, яким чином незаконно нажиті кошти перетворюються на легальні активи.*
3. Цілі розслідування:
   - *Визначення конкретних цілей розслідування, таких як розкриття фінансових злочинів, затримання та припинення діяльності злочинної організації.*
   - *Виявлення основних осіб або подій.*
4. Ще потрібні докази для притягнення до відповідальності:
   - *Визначення інших видів доказів, необхідних для притягнення до відповідальності осіб, які беруть участь в злочинній організації або власників незаконно нажитих активів.*
   - *Аналіз фінансових та немайнових доказів для підтвердження злочинів та виявлення відповідності закону.*
5. Співпраця та обмін інформацією:
   - *Визначення ключових агентств, органів чи команд, які беруть участь в розслідуванні, і забезпечення співпраці та обміну інформацією.*
   - *Узгодження дій та ролей різних структур для ефективного проведення розслідування.*
6. Плани подальших кроків:
   - *Розроблення детального плану подальших кроків та визначення строків та відповідальних за їх виконання.*
   - *Врахування результатів аналізу доказів та планування наступних кроків для досягнення мети розслідування.*

> *Ця схема надає загальний огляд процесу фінансового розслідування, включаючи аналіз структури злочинної організації, фінансових потоків, визначення цілей розслідування, важливість додаткових доказів та плани подальших кроків.*

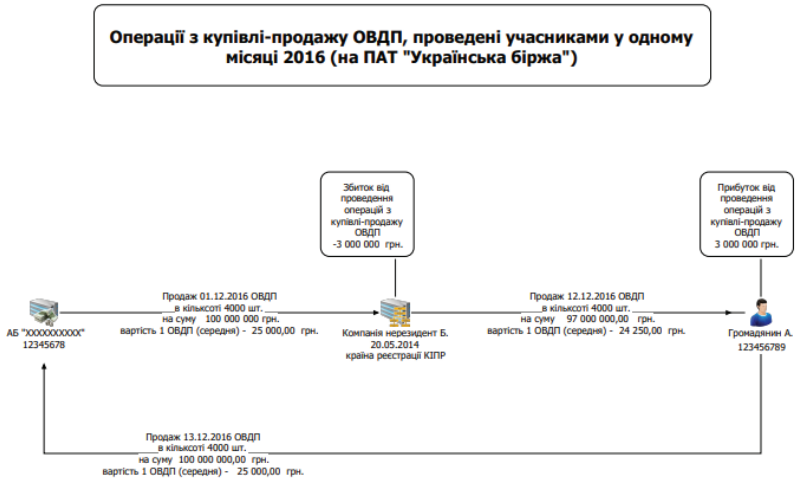
Вона допомагає організувати та систематизувати роботу слідчого з метою досягнення успішних результатів у боротьбі з фінансовою злочинністю.

ПРАКТИЧНІ КЕЙСИ.

Зловживання на ринку цінних паперів. Схема ОВДП.

На офіційному сайті Національного банку України в розділі «Нормативна база» інформація щодо ризиків проведення фінансових операцій з ОВДП, в якому повідомляється, що Національним банком під час здійснення нагляду за банками у сфері фінансового моніторингу виявлено ряд фінансових операцій з цінними паперами, зокрема облігаціями внутрішньої державної позики, що проводились юридичними та фізичними особами, клієнтами банків, характер яких може свідчити про легалізацію доходів, одержаних злочинним шляхом. Особливістю проведення подібних операцій є купівля за більш високою ціною та продаж за більш низькою ціною (тобто зі збитком) ОВДП з таким же ISIN кодом юридичними особами протягом короткого проміжку часу, в тому числі, одного робочого дня, що повторюється неодноразово (циклічно).

Один із прикладів проведення клієнтами наведених фінансових операцій виглядає так: Брокер, діючи від свого імені за рахунок і за замовленням юридичної особи – нерезидента, придбає у банка пакет ОВДП за ринковою ціною. В подальшому, цей брокер продає, а інший брокер придбає зазначений пакет ОВДП, діючи за рахунок і за замовленням фізичної особи, за ціною, що є нижчою від ціни придбання, але при цьому може бути в межах ринкових цін.



Надалі, цей же пакет ОВДП викуповує перший брокер, який діє від свого імені, за рахунок і за замовленням юридичної особи – резидента, за ринковою ціною та знову перепродає на користь фізичної особи, за ціною, нижчою від ціни придбання, але при цьому в межах ринкових цін. Ця фізична особа здійснює подальший продаж зазначеного пакету ОВДП банку за ціною, що є вищою за ціну придбання, але при цьому може бути в межах ринкових цін. За результатами проведення зазначених вище операцій купівлі-продажу пакету ОВДП фізична особа отримує інвестиційний прибуток у розмірі декількох мільйонів гривень, а юридичні особи - інвестиційний збиток у такому ж розмірі.

Так, при проведенні аналізу інформації, яка міститься в базі даних Національної комісії з цінних паперів та фондового ринку, було виявлено, що протягом одного місяця 2016 року особа А укладала правочини пов'язані з купівлею/продажем ОВДП з юридичною особою нерезидентом Б (Республіка Кіпр), за результатом яких особа нерезидент Б отримав збиток, а прибутки особи А від укладених правочинів могли скласти понад 20 млн.грн.

Інформація збиралася на сайті Національної комісії з цінних паперів та фондового ринку: https://www.smida.gov.ua/

Корупційні правопорушення на підприємствах важкої промисловості.

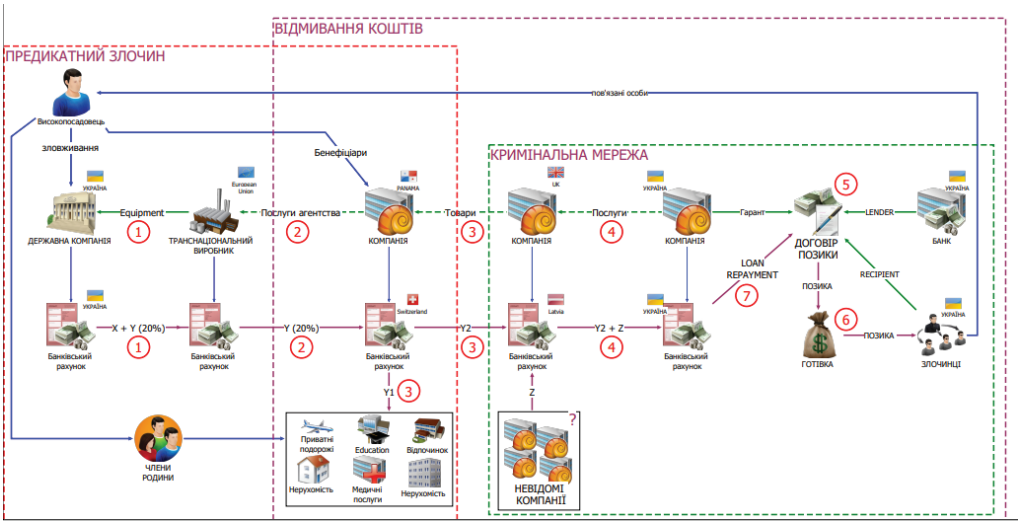
Під час досудового розслідування корупційних дій високопосадовця виявлені ознаки діяльності пов'язаної з ним організованої злочинної групи, яка надавала послуги по відмиванню коштів з використанням фіктивних компаній, зареєстрованих у різних юрисдикціях. Також у схемі легалізації був задіяний фінансовий посередник – банк, підконтрольний цій організованій злочинній групі.

Коротко про предикатний злочин. Високопосадовець досягає домовленості із європейським виробником обладнання щодо закупівлі продукції державним підприємством із врахуванням 20% надбавки (на схемі X - це вартість обладнання, Y - надбавка, що становить його особистий інтерес.

Європейський виробник, будучи зацікавленим в підписанні контрактів з державним підприємством погоджується сплатити 20% надбавку (на схемі позначено як Y) у якості агентських послуг на рахунок панамської компанії, відкритий у Швейцарії, відповідно державне підприємство укладає договір із європейським виробником за завідомо завищеними на 20% цінами. У подальшому після отримання європейським виробником від українського державного підприємства коштів 20% від

них скеровувалось на рахунок Панамської компанії. В ході розслідування було встановлено, що бенефіціаром швейцарської компанії є безпосередньо високопосадовець.

Одержані кошти було частково використано для забезпечення потреб членів родини високопосадовця – на купівлю та оренду нерухомості в Європі, оплату медичних та туристичних послуг членів родини високопосадовця тощо (на схемі позначено як Y1), що по суті вже є легалізацією.



У подальшому з рахунку у Швейцарії основну частину коштів (на схемі позначено як Y2) під виглядом оплати обладнання, високопосадовцем було спрямовано на латвійський рахунок британської компанії. Зазначена компанія, по-суті, є майданчиком для відмивання коштів міжнародною злочинною групою.

Було встановлено, що на рахунки британської компанії акумулювалися значні фінансові ресурси із різних джерел – кошти на цей рахунок надходили з розрахункових близько 50 компаній (на схемі позначено, як Z). В подальшому акумульовані на рахунки британської компанії кошти (на схемі позначено як Y2+Z) під виглядом оплати товарів і послуг було перераховано на рахунок української компанії.

З метою переведення коштів у готівку кримінальна група використала фінансового посередника – український банк. Одночасно з переведенням коштів з британської на українську компанію підконтрольний організованій групі банк укладає фіктивні кредитні договори (5) із рядом фізичних осіб, за якими з каси банку видаються готівкові кошти (6).

Поручителем за кредитними договорами виступила українська компанія (саме та, на рахунки якої надходили кошти з британської компанії), яка і через день після видачі кредитів банком, як поручитель погашає заборгованість перед банком за відповідними кредитними договорами. *Таким чином відбувся «розрив ланцюга» та легалізація коштів.*

Зверніть увагу, що частина осіб, які отримали кошти готівкою, є пов'язаними особами із високопосадовцем. Таким чином, коло замикається. Легалізацію коштів високопосадовця із коштами з інших джерел було легалізовано через ряд фіктивних фірм, зареєстрованих у різних юрисдикціях із залученням послуг фінансового посередника – банка.

Інформація збиралася у майже всіх державних реєстрах, адміністраторами яких є державні органи, до яких є доступ у правоохоронних органів, аналізувалися банківські виписки, було використано інструмент запиту в рамках міжнародної правової допомоги, матеріали Держфінмоніторингу.

Зловживання владою для отримання неправомірної вигоди.

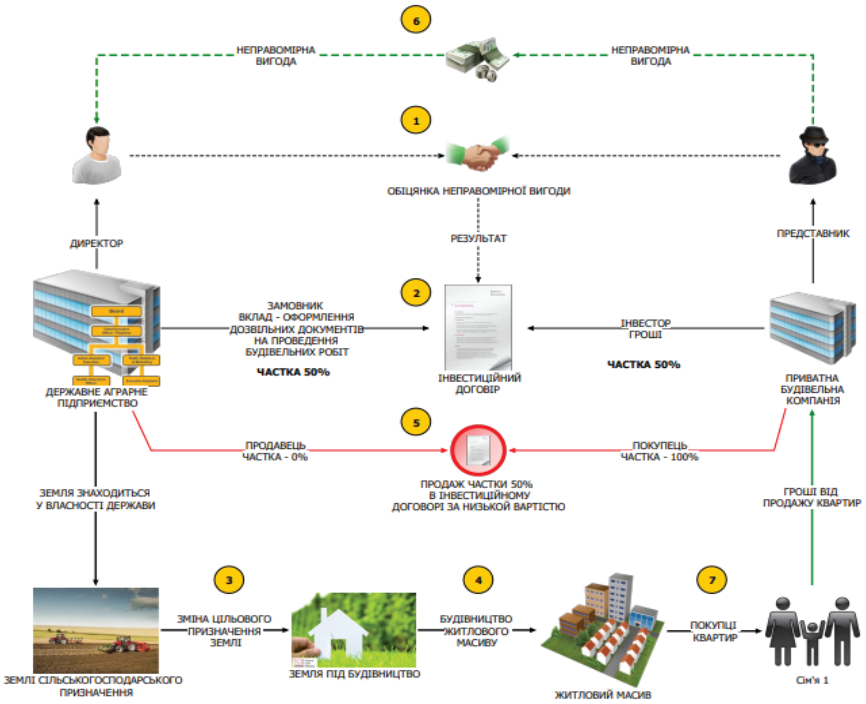
Директор Державного аграрного підприємства з метою одержання неправомірної вигоди від представника приватної будівельної компанії від імені Державного аграрного підприємства уклав інвестиційний договір з цією компанією.

Внеском у інвестиційний договір від імені Державного аграрного підприємства з часткою 50% було оформлення дозвільних документів на проведення будівельних робіт на землі сільськогосподарського призначення, яка знаходилася у власності держави.

В подальшому директор Державного аграрного підприємства від імені цього підприємства продав частку Державного аграрного підприємства у інвестиційному договорі будівельній компанії за вартістю нижче ринкової і отримав обіцяну неправомірну вигоду.

Гроші, які були передані директору Державного аграрного підприємства, були генеровані від продажу квартир житлового масиву, який побудували на землі, призначення якої було змінено з сільськогосподарського призначення на будівництво багатоквартиних будинків.

Для виявлення схем и було проведено аналіз документації забудовника, укладені угоди, аналіз фінансових операцій будівельної компанії та виписок по банківських рахунках директора Державного аграрного підприємства.



DOI: https://doi.org/10.36486/978-966-2310-66-5-32

Сучасний аналітик злочинності повинен вміти писати й публікувати з такою ж майстерністю, з якою він розраховує та аналізує

Christopher W. Bruce (IACA)

РОЗДІЛ 32
Аналітичні продукти

Наталія Свиридюк
Юрій Кардашевський

Результатом діяльності аналітика є аналітичний продукт, який характеризується значною різноманітністю – від щоденних оглядів, щомісячних статистичних звітів до щорічних аналітичних звітів.

Після того, як аналітик зібрав інформацію – про серію, закономірність, тенденцію, проблему або іншу тему щодо аналізу злочинності – у нього є кілька варіантів, як передати її співробітникам поліції. Приклади включають особисті брифінги, радіопереговори, електронні листи, тематичні бюлетені або попередження, а також періодичні звіти. Вибір одного варіанту не виключає інших; аналітики повинні використовувати різні методи, щоб переконатися, що їхня аудиторія отримає повідомлення.

«Аналітик, який виявляє та аналізує серію пограбувань цілодобових магазинів, може почати з короткого повідомлення електронною поштою до відповідних підрозділів про існування та ключові ознаки цієї серії. Потім він може домовитися про короткий виступ на нараді у підрозділі, де він презентує стислий, але детальний бюлетень про цю серію. Наступного ж дня, заганяючи в кут керівника підрозділу, запитує: «Ви бачили мій бюлетень? Мені цікаво, чи є у вас якісь думки...» і перераховує ключові моменти. Таке поєднання письмового та усного, високотехнологічного й менш технологічного підвищує шанси на те, що всі члени підрозділу отримають повідомлення у найкращий для них спосіб [1]».

> *Найретельніший, найглибший аналіз – години ваших розумових зусиль - зів'яне у кошику для сміття, якщо цільова аудиторія не захоче його читати. Навіть якщо бюлетень або інший продукт буде прочитаний, він не матиме жодного впливу на злочинність, якщо його читачі не довіряють йому, не розуміють і не сприймають його (IACA) [1].*

Водночас конкретні аналітичні продукти, що використовуються в окремому правоохоронному органі, агентстві, визначаються відповідними юридичними документами (щодо їх видів, структури та змісту), можуть залежати від традицій, уподобань персоналу аналітиків, потреб агентства, а також вимог внутрішньої політики.

Важливо звернути увагу на те, що результати аналітичної діяльності можуть бути подані або презентовані у двох ключових формах:

- *брифінг (коротка усна презентація ключових елементів ситуації або аналізу для конкретної аудиторії);*
- *письмовий звіт.*

Усний брифінг є найбільш ефективним, коли він використовується для представлення огляду аналізу, який стане основою для негайних дій, наприклад, у критичних ситуаціях, що швидко змінюються. Ефективна презентація може суттєво вплинути на сприйняття аналітичного продукту.

Основна перевага усного брифінгу полягає в тому, що він забезпечує безпосередню взаємодію між користувачами аналітичних висновків та аналітиками – виконавцями аналізу. Продукти аналізу можуть бути складними; ефективна усна презентація дає можливість представити висновки в чіткій логічній послідовності, крок за кроком. Тому дуже важливо, щоб брифінги відображали логічне обґрунтування, яке було використане в аналізі.

Усні брифінги мають три основні переваги:

Економія часу – максимальна кількість інформації може бути передана за найкоротший час.

Прямий контакт – усний брифінг забезпечує прямий контакт між аналітиком і клієнтом. Це створює можливість для динамічного опитування джерел даних, оцінки надійності даних,

висновків та їхньої вірогідності тощо. І клієнт, і аналітик можуть використовувати цю можливість, і аналітик може скористатися цією можливістю, щоб переконатися, що проект просувається в правильному напрямку і дає дієві результати. Маючи прямий контакт, користувач може точніше оцінити важливість результатів аналізу в контексті їхнього зв'язку з іншою з іншою інформацією на цю тему.

Динамічність – усний брифінг може бути переглянутий в останній момент, щоб включити актуальну інформацію. Він може повідомляти про розвиток проєкту майже в режимі реального часу. Брифінг може, по суті, бути описом ситуації, що склалася безпосередньо перед брифінгом.

Усні брифінги, як правило, включають значну частку імпровізації та мислення на місці. Однак підготовка все одно необхідна, оскільки для досягнення бажаного результату брифінг має відбуватися за заздалегідь розробленим сценарієм.

> *Для початку завжди важливо проаналізувати аудиторію – для чого буде використана інформація, надана під час брифінгу? Який рівень знань аудиторії? У чому полягають її інтереси?*

Ретельна підготовка та логічна презентація є запорукою ефективності усного брифінгу. Логічні міркування, які були використані в аналізі, повинні бути очевидними під час брифінгу.

Наразі значну частину поширення розвідувальної аналітичної інформації складають письмові звіти [2]. Письмовий звіт – це презентація ключових елементів ситуації або аналізу для певної аудиторії. Аудиторія може варіюватися від патрульних, яким потрібна лише невелика доповідь, до старших офіцерів, яким потрібні більш глибокі звіти, або до колег, яким може знадобитися все. Звіт є найефективнішим, коли він використовується для представлення огляду аналізу, який може стати основою для майбутнього плану дій, – наприклад, коли час не є вирішальним фактором, що впливає на потенційну операцію.

> *Важливо пам'ятати, що письмовий звіт створює мало можливостей для прямого зворотного зв'язку.*

Коли його читають, він повинен передати власну цінність і вказати на відповідні висновки. Можливості щось додатково пояснити, як під час усної презентації, вже не буде. Це означає, що письмові звіти повинні бути професійно оформленими, оскільки, як тільки вони потрапляють до рук читача, починають впливати на нього. Розумний, кольоровий, чіткий брифінг-аркуш, швидше за все, буде ефективнішим, ніж довгий неохайний текстовий аркуш.

Звіти повинні бути вичитані як для точності, так і для чіткості викладу, якщо можливо. Це підвищує довіру до звіту й допомагає забезпечити правильне донесення повідомлення.

Існує кілька переваг і недоліків подання письмового звіту замість усного брифінгу [2].

Переваги:

- ✓ *звіт може бути адаптований до потреб конкретного одержувача, таким чином опускаючи інформацію, яка не є релевантною та/або неважливою для потреб цієї особи;*
- ✓ *зміст звіту можна перечитати на дозвіллі та виокремити ключові моменти для подальшого використання;*
- ✓ *до змісту звіту можна повертатися (під час обміну ідеями або додатковою інформацією);*
- ✓ *легкість для подальшого розповсюдження.*

Недоліки:

- ✓ *автор звіту повинен знати аудиторію, щоб оптимізувати зміст звіту; інакше йому доведеться включати в нього стільки деталей, скільки йому відомо на цей момент;*
- ✓ *після написання звіт стає історичним документом, моментальним знімком ситуації, що стосується інформації, яка є в наявності на той момент;*
- ✓ *через відстань між автором і читачем неминуча затримка в обміні інформацією між ними;*
- ✓ *його поширення не так легко контролювати.*

Розробляючи продукт аналізу злочинності, необхідно враховувати як мету, так і аудиторію продукту [3]. Аналітичні продукти щодо злочинності можуть слугувати багатьом цілям: від інформування громадян про нещодавні події, допомоги правоохоронним органам у плануванні, до затримання підозрюваного злочинця. Наприклад, щомісячні карти міста, на яких зображені зареєстровані злочини, корисні для надання громадськості загальної інформації про зміни в «гарячих точках» зареєстрованих злочинів; однак детальна карта кожної «гарячої точки» може бути необхідною для

патрульних та слідчих, яким потрібна конкретна інформація, щоб зосередити свої зусилля на вирішенні проблем. У будь-якому випадку, важливо підготувати карти, які відповідають поставленій меті.

Крім того, існує багато зацікавлених сторін щодо аналітичних продуктів про злочиність. Це можуть бути співробітники поліції, широка громадськість, громадські групи, керівництво шкіл або члени міської ради. Визначивши потреби, очікування та рівень кваліфікації цих осіб, можна розробити продукти, які підходять для кожної групи. Наприклад, карта місць проживання всіх відомих членів угруповання з іменами та номерами справ може бути корисною для правоохоронців, які збирають розвідувальну інформацію про угруповання. Однак карта з таким рівнем деталізації не буде поширюватися серед громадськості, оскільки це може порушити права особи на приватне життя або скомпрометувати розслідування. Може бути доречним нанести на карту коротке позначення, наприклад, «тільки для використання правоохоронними органами» або «зовнішнє використання», щоб вказати на цільову аудиторію. Також під час створення аналітичного продукту потреби користувачів інформації повинні бути збалансовані з політичними, правовими та етичними міркуваннями.

Аналітичні продукти поділяються на періодичні, які створюються на відповідну дату протягом встановленого періоду, та такі, що створюються за потребою або на запит замовника аналізу. Зокрема за змістом, аналітичні продукти можуть поділятися на [4]:

> ***Аналітичний звіт*** *– це аналітичний продукт, що містить обґрунтовані відповіді на запитання, поставлені замовником аналізу, які стали предметом аналітичного дослідження, зокрема результати оцінки ризиків та загроз безпеки, пропозиції щодо їх мінімізації та усунення.*
>
> ***Досьє*** *на фізичну або юридичну особу, об'єкт (предмет), організовану групу чи злочинну організацію, подію – це документ інформаційного характеру відносно об'єкта дослідження відповідно до запиту замовника, що містить систематизовану інформацію, сформовану у вигляді, що дозволяє її подальше використання уповноваженими особами, зокрема для проведення аналітичного дослідження та може бути його невід'ємною частиною.*
>
> ***Профіль*** *– аналітичний продукт, який уміщує типові або, встановлені у ході аналізу ознаки, критерії, які дають змогу за комплексом цих ознак охарактеризувати та встановити потенційну жертву, злочинців, подію.*
>
> ***Аналітичні документи*** *(довідки, інформаційні зведення, аналітичні огляди) – аналітичні продукти, які готуються залежно від поставлених завдань та обсягів інформації за усіма напрямами діяльності підрозділу.*
>
> ***Аналітичне орієнтування*** *– аналітичний продукт, який містить відомості про вчинене правопорушення, яке було виявлено у процесі проведення аналітичного дослідження інформаційних ресурсів, наданих замовником або ініціативно.*

Інтерпол для підтримки своїх підрозділів та правоохоронних органів у країнах-членах зазначає щодо можливості створення різноманітних аналітичних продуктів, зокрема [5]:

- ✓ *аналітичні звіти;*
- ✓ *оцінка загрози для регіонів або конкретних злочинів;*
- ✓ *оцінка ризику для конкретної події;*
- ✓ *розвідувальні аналітичні публікації (бюлетені, щомісячні звіти).*

Зокрема, звіти Інтерполу зі стратегічного аналізу забезпечують широку оцінку конкретної кримінальної загрози, або тенденції, або злочинної поведінки в конкретному середовищі. Вивчаються різні фактори, які впливають на різні види злочинів. Це дозволяє оцінити можливі тенденції злочинності в найближчому або середньостроковому майбутньому (тобто ескалація або деескалація). Аналітичні звіти стратегічного характеру включають оцінку загроз і ризиків (для конкретного регіону, злочину або події), звіти про тенденції злочинності, звіти про сканування навколишнього середовища та раннього запобігання.

Аналітичний продукт містить докладний опис проведених досліджень та зроблених за їх результатами висновків, обґрунтованих відповідей на запитання, поставлені замовником, або запитання, поставлені самим аналітиком під час проведення аналізу.

З точки зору розгляду продуктів інформаційно-аналітичної діяльності як інформаційного базису для прийняття управлінських рішень можливо використати таку класифікацію [6]:

Документи інформаційного характеру.

Відрізняються такими загальними особливостями: інформують щодо предмета, тобто за характером є первинними (без поглибленого аналізу) та масовими документами, тому повинні складатися максимально лаконічно та точно. Документи інформаційного характеру дозволяють швидко отримати

адекватну інформацію, що дає можливість прийняти попереднє рішення. Про інформування щодо типового, в загальному плані відомого предмета спочатку надається загальна характеристика, а потім, в порядку спадання важливості, – найбільш суттєві параметри. Якщо предмет викладення нетиповий, новий, то інформування краще здійснювати від часткового до загального. Такі документи зазвичай надані у вигляді довідок, зведень.

Документи аналітичного характеру.

Їх особливістю є дослідноопроблемний характер. Від інформаційних повідомлень їх відрізняє комплексна мета: описати, роз'яснити, відпрацювати рішення, обґрунтувати. Такі документи зазвичай складаються у вигляді довідок, статей, оглядів, звітів.

Довідка – це документ, який вміщує в себе аналіз значень показників інформаційного поля (тобто масиву інформації, який складається навколо об'єкта моніторингу) з точки зору визначеної проблеми. *За змістом та метою довідки можна класифікувати наступним чином [6]:*

Інформаційні довідки: про факти, пригоди, події (мета – ідентифікація предмету повідомлення; повідомлення вузько спрямовані та тематично однорідні); про ситуації, обстановку (ідентифікують ситуацію; до викладення умов, результатів та наслідків додається опис тенденції розвитку); про явища, процес (важливе викладення просторово-часового аспекту, типізація явища, виявлення тенденцій, результатів та наслідків його розвитку); про дії, заходи, роботу (змістовні характеристики діяльності, учасників, результати та наслідки); про організацію або особу (змістовний та багатоаспектний предмет інформування.

Аналітичні довідки: аналітична довідка щодо управлінських проблем (присвячена висвітленню, аналізу та пропозиціям щодо вирішення управлінських проблем); висновки (довідка) за результатами перевірки, обстеження (складається за результатами контрольно-перевірочних заходів).

Інформаційно-аналітична записка – стислий та чіткий опис проблеми або виконаної роботи.

Аналітичний огляд призначений для швидкого ознайомлення та комплексного вивчення складних предметів. Складання оглядів вимагає високої предметної та інформаційно-методичної кваліфікації працівників інформаційно-аналітичних підрозділів. Крім «оглядовості» та «стислості», такі документи мають ще й аналітичний аспект, що пов'язаний з аналізом, порівнянням різних точок зору та формуванням обґрунтованих оцінок. Таким чином, аналітичні огляди (на відміну від довідок та статей) мають комплексний та місткий характер.

Доповідь – це документ, якій містить викладення певних питань, висновків, пропозицій та призначений для усного читання. Доповідь передбачає не тільки перерахування параметрів проблеми та формулювання висновків, але й внесення пропозицій щодо вирішення питання.

Інформаційне зведення про події, пригоди, обстановку являє собою зведену воєдино за визначений часовий період у відношенні визначеного об'єкта (території, структури, галузі) інформацію про події, що відбулися, особливості обстановки, стан справ.

Аналітична стаття – це стаття, яка містить аналіз діяльності об'єкта моніторингу. Вона повинна містити у собі велику кількість фактів, що аналізуються та визначати їх взаємозв'язок. Стаття, з одного боку має бути доступна для розуміння широкому загалу читачів, а з іншого боку – бути цікавою для фахівця в галузі, що досліджується.

Аналітичний звіт – це аналітичний продукт, в якому описано сукупність показників за якими оцінюється інформаційне поле об'єкта моніторингу. Він складається з діаграм, графіків та таблиць, що супроводжуються стислими або розгорнутими аналітичними довідками. Заключна частина звіту зазвичай відображається у вигляді основних висновків та рекомендацій.

Окремо важливо зазначити, що метою ***звітів стратегічного аналізу*** є підтримка прийняття обґрунтованих рішень та планування заходів. Залежно від вимог і цілей можна підготувати різні типи документів [1]:

Повідомлення раннього виявлення/розвідувальні аналітичні повідомлення висвітлюють нові або нещодавні зміни, тенденції та події у середовищі, які можуть бути тематичними чи географічними. Основна мета полягає в тому, щоб описати зміни та оцінити можливий вплив на кримінальні ринки, ситуацію з безпекою та суспільство або більш широку географічну територію. Такі сповіщення є короткими та конкретними, спрямованими на проактивне та швидке інформування одержувача про нову зміну чи тенденцію, а також коротко вказують на очікувані наслідки цієї зміни чи тенденції.

Оцінюванням загрози аналізується та визначається рівень загрози кримінального явища. Вони можуть зосереджуватися на організованих злочинних групах, конкретних злочинних зонах або регіонах. Оцінки зазвичай мають середньо- та довгостроковий характер та орієнтовані на майбутнє. Вони надають особам, які ухвалюють рішення, стратегічну інформацію та рекомендації.

Звіти з оцінки ризиків описують визначений рівень потенційних ризиків, де оцінка ймовірності, впливу та відповідних вразливостей додається до оцінки загрози.

Ситуаційні звіти мають переважно описовий характер. Їх мета – надати детальний огляд певної теми. На відміну від оцінки загроз, вони, як правило, не містять рекомендацій щодо дій та обмежуються фактичними висновками. Вони можуть зосереджуватися на різноманітних темах, від певної кримінальної сфери чи способу вчинення до певної злочинної групи чи географічного регіону.

Повнота аналітичного продукту визначається дотриманням так званих «**7 золотих питань**» або «**питань розкриття**» [4]. Важливо, щоб вони застосовувалися у різній часовій перспективі, тобто питання «*Що?*» або «*Хто?*» мають бути поставлені у таких формах:

- ***що** відбулося?* або ***що** може відбутися?;*
- ***хто** обвинувачується (виконавець)?* або ***хто** може бути винуватим (виконавцем)?*

7 золотих питань:

1. ***Що?** (що відбулося?, що може відбутися?, якими були / є / будуть наслідки цієї події?*);
2. ***Де?** (де відбулося?, де це може статися?)*;
3. ***Коли?** (коли це відбулося?, коли це може статися?);*
4. ***Чому?** (чому це відбулося?, чому це може статися?);*
5. ***В який спосіб?** (у який спосіб це було вчинено?, за допомогою яких методів це може бути вчинено?);*
6. ***За допомогою чого?** (якими знаряддями це було вчинено?, що може бути використане для вчинення цього?);*
7. ***Хто?** (хто це вчинив?, хто може це вчинити?).*

Відомий в Україні фахівець з кримінального аналізу Юрій Крутік зазначає, що основними вимогами, які висуваються до аналітичного матеріалу підготовленого в процесі обробки такої інформації, слід вважати вимоги [6], які висуваються до доказів у кримінальному провадженні (статті 84, 85 Кримінального процесуального кодексу України), оскільки кінцевою метою роботи аналітика підрозділу кримінального аналізу повинне бути спрямування на практичне використання результатів його діяльності, а саме:

належність отриманої інформації – тобто відношення відомостей до об'єкта аналітичного дослідженні;

допустимість отриманої інформації – тобто використання для аналітичного дослідження відомостей отриманих виключно в порядку, що не суперечить законодавству, а в окремих випадках – лише тієї інформації, яка була отримана відповідно до процесуальних вимог та правил;

достовірність отриманої інформації – тобто використання для аналітичного дослідження відомостей, істинність та точність яких не викликає сумнівів;

достатність отриманої інформації – тобто використання для аналітичного дослідження такої сукупності відомостей, на основі яких може бути зроблений певний висновок (ймовірний чи достовірний) та прийнято відповідне рішення (проміжне або кінцеве);

оперативність обробки отриманої інформації – це мінімально необхідний час для всебічного вивчення необхідного обсягу матеріалу, та підготовки кінцевого аналітичного продукту.

Вивчаючи історичні аспекти щодо розуміння в правоохоронному середовищі принципів, структури та змісту аналітичних розвідувальних продуктів, Фрост і Морріс ще у 1983 році у своєму посібнику «Звіти поліцейської розвідки» запропонували чіткий формат для збору сирих даних, які можуть бути відправною точкою у процесі підготовки «обробленої розвідувальної інформації» (7). Звісно, що цей процес не стоїть на місці, постійно розвивається і доповнюється складовими та характеристиками новаційних рішень і підходів. Свого часу Фрост зазначав: *«Звіти - це джерело життєвої сили розвідувального аналітичного процесу» [8, с. 181]*.

Відомий фахівець, професорка Редфордського університету Рейчел Боба Сантос (Rachel Boba Santos) наводить деякі загальні типи продуктів аналізу злочинності [3]:

Бюлетені про злочинність. Короткі документи на одну-дві сторінки, які описують тактичну короткострокову тенденцію або закономірність.

Службові записки. Документ у формі листа, який підсумовує запит, пояснює аналіз, висвітлює цікаві результати і, в деяких випадках, дає рекомендації щодо реагування або подальшого аналізу. Вони повинні бути включені як супровідні листи до досліджень та спеціальних звітів.

Щотижневі/щомісячні/щоквартальні звіти та карти. Документи та карти які передають ту саму інформацію через регулярні проміжки часу, щоб інформувати про діяльність і дозволяють виявляти проблеми. Ці продукти повинні бути послідовно відформатовані, щоб забезпечити впізнаваність для замовників та можливість порівняння.

Річні звіти. Звіти, які надають інформацію, агреговану за роками та публікуються на щорічній основі. Вони мають включати розбивку за географією, місяцями та типами діяльності (наприклад, типи злочинів, типи викликів та нещасні випадки), а також порівняння між роками. Вони також можуть включати порівняння з іншими подібними юрисдикціями, а також з державними та національними показниками на державному та національному рівнях.

Звіти про дослідження. Звіти, що містять опис даних, методологію та аналіз дослідницького проєкту (наприклад, проєкту з вирішення проблеми або оцінки програми), а також результати аналізу, інтерпретацію отриманих результатів та рекомендації щодо реагування або майбутніх досліджень.

Спеціальні звіти. Це звіти, які розробляються на спеціальній основі й стосуються конкретної проблеми, наприклад, дорожньо-транспортних пригод біля шкіл або ефективного розподілу нового підрозділу поліцейських. Аналіз, на основі якого складаються ці звіти менш ретельний, ніж у дослідницьких звітах, і, відповідно, займає менше часу. Ці спеціальні звіти складають більшу частину щоденної роботи аналітика з питань злочинності. Ці загальні категорії можуть включати інформацію про злочини, виклики, арешти та нещасні випадки. Вони також можуть бути специфічними для певної території, наприклад, вулиці, кварталу, дільниці, району або всього міста. Інші, більш специфічні типи можуть включати списки інцидентів, інформацію про банди, оголошення про зниклих безвісти та зведення за картами розшуку.

Узагальнюючи підходи до підготовки аналітичних продуктів у виданні Управління по наркотиках та злочинності ООН (*United Nations Office on Drugs and Crime* (UNODC)) [2] визначено, відповідно 10 стандартів:

1. *Проаналізовані дані повинні використовуватися для спрямування правоохоронних операцій та розслідувань*
2. *Аналіз має бути невід'ємною частиною кожного великого розслідування, яке проводить агентство.*
3. *Аналітичні продукти повинні містити, як мінімум, письмовий звіт. Візуальні продукти також можуть бути представлені, але вони є прийнятними лише як доповнення до письмового звіту, а не як його заміна.*
4. *Аналітичні продукти повинні містити висновки та рекомендації. Вони подаються на розгляд керівництву для прийняття рішень.*
5. *Розробка аналітичного продукту вимагає застосування аналізу даних. Компіляція даних, яка не відображає порівняння або інші міркування, не є аналізом.*
6. *Аналітичні продукти мають бути точними. Користувачі повинні мати можливість покладатися на дані, надані їм аналітиками.*
7. *Аналіз має бути своєчасним.*
8. *Аналітичні продукти повинні відображати всі релевантні дані, доступні з будь-яких джерел і засобів, доступних аналітику.*
9. *Аналіз повинен включати найкращі та найсучасніші комп'ютерні програми, компіляцію, візуалізацію та аналітичні методи, доступні аналітику, візуалізації та аналітичні методи, доступні в середовищі аналітика.*
10. *Аналіз повинен відображати і оцінювати якісний і кількісний внесок аналітика у виконання місії та пріоритетів установи чи організації, для якої вони аналізуються.*

Варто звернути увагу й на інші застереження щодо правил написання розвідувальних звітів [9]:

- *чіткість та лаконічність – неточні твердження або помилки в розрахунках підірвуть вплив звіту;*
- *написання тексту від третьої особи;*
- *уникнення використання професійного жаргону;*
- *підтримка логічного потоку думок, ідей та аргументів;*
- *відслідковування правильності написання та граматики (орфографічні помилки відволікають читача, а у випадку з іменами та особами можуть призвести до плутанини).*

Таким чином, звіт повинен містити найважливіші результати, висновки та рекомендації. Як і усна презентація, письмовий звіт повинен передавати результати аналізу простою мовою та визначати

моменти, на яких необхідно наголосити. Зміст повинен бути чітким, лаконічним, добре надрукованим і розділеним інтервалами, уникаючи довгих друкованих блоків.

Дуже корисною структурою для написання розвідувальних звітів є ***перевернута піраміда***.

> *Щоб використовувати її, необхідно уявити, що кожен абзац звіту – це піраміда, що стоїть догори ногами на вершині. Найважливіша ідея повинна бути в найширшій частині піраміди – в головному реченні, а всі інші ідеї в цьому абзаці підтримують цю головну ідею. Насправді, речення, які слідують за основним реченням треба розташовувати в порядку зменшення їхньої важливості.*

Аналогічно, весь аналітичний звіт можна розглядати як перевернуту піраміду. Найбільш найважливіша інформація повинна бути на початку, а не в кінці. Якщо цей перший розділ достатньо переконливий, читач продовжить читання. Існує твердження, що читач хоче спочатку дізнатися «головну ідею» – головна ідея – це висновок. Деякі автори притримують головну ідею до кінця звіту, ніби чекаючи на кінець історії, щоб розкрити «кульмінацію». В аналітичному звіті має бути навпаки. Спочатку подається основна ідея, а вже потім історія – деталі, які підтверджують висновки.

Якщо застосовувати цей принцип в усьому звіті – в організації звіту, розділах звіту та абзацах у кожному розділі – звіт буде легше писати, а також легше читати.

Відповідно до цього підходу, резюме можна побудувати, зібравши в послідовності тематичних речень перші три-чотири абзаци. Хоча може знадобитися деяке переписування, щоб уникнути повторень і досягти динамічного читання, такий спосіб структурування резюме часто є ефективним.

Компоненти аналітичних продуктів

Аналітичний продукт може включати один або декілька типів аналітичних результатів, які можуть включати таблиці, діаграми, графіки, карти, зображення та описи. В одному аналітичному продукті слід використовувати баланс одного або декількох з цих компонентів, а включення всіх або тільки одного компонента слід уникати. Наприклад, двосторінковий нарис про нещодавні крадіжки зі зломом не буде таким же ефективним, як простий опис схеми, таблиця з відповідною інформацією, графік із зазначенням часу доби та дня тижня, коли мала місце протиправна діяльність, а також карта, яка вказує на місце, де ця діяльність відбувається. І навпаки, продукт аналізу злочинів не повинен містити лише карту або графік [3]. Незважаючи на те, що карта або діаграма повинні бути створені самостійно, аналітик повинен також включити додаткову інформацію, таку як цікаві знахідки, інтерпретація результатів та рекомендації для подальшого аналізу.

Структура аналітичного звіту [2]

Обкладинка з назвою. На титульній сторінці, окрім назви, вказується ім'я аналітика, підрозділ і дата написання звіту. Заголовок повинен одразу привертати увагу. Також, якщо документ має обмежений доступ, це має бути зазначено.

Зміст звіту. Він є необхідним в більшості випадків, особливо якщо в документі є велика кількість діаграм, додатків тощо.

Передмова/методологія. Передмова є короткою і містить детальну інформацію про тип проведеного аналізу, використані методи, мету аналізу, команду, яка проводила аналіз, і, якщо це доречно, – інформацію про те, для кого він проводився, детальну інформацію про періоди, охоплені аналізом. Крім того, вказується ключ до будь-яких методів, використаних для виділення фрагментів тексту, а також ключ усіх символів, використаних для представлення об'єктів і зв'язків у аналітичних діаграмах.

Підсумок або огляд. Розширення висновків зазначених в резюме, але викладається коротко та включає огляд результатів, що ґрунтуються на гіпотезі й висновках, передумов і рекомендацій.

Основний звіт. Передумови та інформація, з якої вони були отримані, стають основними розділами звіту. Вони повинні бути короткими й логічно описувати структуру аналізу, починаючи з висновку, в якому викладено результати всіх використаних передумов. Потім передумови описуються й підкріплюються відповідними розвідувальними даними, а також невеликими діаграмами такими як діаграми зв'язків тощо. Рекомендується звертати увагу на висновки та аналітичні коментарі (наприклад, висвітлення прогалин щодо аналітичнихданих та інформації) за допомогою таких методів, як виділення їх рамками використання іншого кольору фону для тексту в кожному конкретному випадку. Фотографії також можуть бути включені до цього розділу, хоча слід пам'ятати, що занадто велика кількість фотографій може ускладнити подальше розповсюдження звіту.

Висновки/рекомендації. Заключний розділ звіту може включати повторення вибраних висновків, а також перелік та обґрунтування рекомендацій на результатах аналізу.

Прогалини щодо аналітичних даних та інформації. У деяких аналітичних звітах надзвичайно корисно перерахувати прогалини щодо використаних даних в окремому розділі, згрупувавши їх так, щоб у перспективі заповнити відповідні прогалини. Це дає змогу користувачам звіту ініціювати й перевіряти ці прогалини.

Додатки. Цей заключний розділ призначений для включення будь-яких великих або додаткових діаграм, які графічно відображають зміст звіту графічно.

Ця модель призначена для того, щоб допомогти аналітику скласти документ, який досягає поставленої мети, тобто іншими словами, передати результати аналізу в найчіткіший, найкоротший і найлогічніший спосіб, наскільки це можливо.

Структура й подача будь-якої презентації, як письмової, так і усної, має бути такою, щоб створити максимальний ефект. Це вимагає від її творця уяви та оригінальності. Аналітики розвивають ці здібності з практикою та досвідом.

Методи поширення

Методи розповсюдження продукту за своєю суттю залежать від його призначення та аудиторії. Вони також покладаються на наявні засоби та технології. Наприклад, аналітик може захотіти повідомити патрульних, що в певній частині міста відбуваються випадки сексуального насильства, і надати їм детальну інформацію [3]. Аналітик, звичайно, не буде надавати цю інформацію в інтернеті для загального огляду, але замість цього він може включити вибрану інформацію на листівки, які роздаватимуть на брифінгах, або розіслати електронною поштою по всьому відомству (внутрішньою) або взяти участь у брифінгах поліцейських, які працюють у тих районах. Таким чином, мета – інформування патрульних у певному районі – диктує спосіб поширення цієї інформації.

Аналітик також повинен розглянути питання про те, який метод поширення інформації є найбільш ефективним і дієвим, оскільки часто найпростіший метод не є найефективнішим. Найефективніший спосіб поширення інформації залежить від поточних конкретних обставин й аналітик повинен постійно звертати увагу на те, що є доречним та ефективним.

Оцінка корисності продуктів аналізу та картографування злочинності

Механізм зворотного зв'язку для аналітичних продуктів важливий для визначення як їхньої актуальності, так і ефективності. Опитування користувачів, неформальні обговорення та/або фокус-групи можуть бути використані для того, щоб дізнатися, чи служить продукт своєму призначенню і чи є корисним для своєї аудиторії. Крім того, самим аналітикам необхідно переглядати та переоцінювати поточні продукти аналізу злочинності. Зміни у фокусі відділу, можливості клієнтів, характер злочинної діяльності та інформаційні технології це лише деякі з факторів, які можуть вплинути на потреби й цілі аналізу злочинів.

Зрештою, важливо пам'ятати і не скотитись до певного анахронізму. Здається дивним коли аналітична система застосовує найкраще, що є в електронній ері, для аналізу інформації, а потім створює лише громіздкі друковані документи. Запитання – це тому, що особи, які приймають рішення, є анахронізмом, чи тому, що система аналітичної розвідки є анахронізмом? [10]

ВИКОРИСТАНІ ДЖЕРЕЛА

1. 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.
2. UNODC. Criminal Intelligence: Manual for Analysts (2011). Publishing production: English, Publishing and Library Section, United Nations Office at Vienna.
3. Rachel, Boba (2001). *Introductory Guide to Crime Analysis and Mapping*. Office of Community Oriented Policing Services U.S. Department of Justice.
4. Користін О., Кирилюк О. Основи аналітичної розвідки в системі державної безпеки: навчальний посібник. Київ: НА СБ України, 2023. 144 с.
5. INTERPOL. https://www.interpol.int/How-we-work/Criminal-intelligence-analysis2
6. Кіреєва О.С., Крутік Ю.В., Махлай О.М., Треус А.С. Основи кримінального аналізу: теорія та практика застосування в оперативних підрозділах Державної прикордонної служби України: навчальний посібник. Хмельницький: Вид-во НАДПСУ, 2022. 388 с.
7. Frost, Charles C. & Jack, Morris (1983). *Police Intelligence Reports*. Orangevale, CA: Palmer Enterprises.
8. Frost, Charles (1990). *Intelligence Report Writing, Criminal Intelligence Analysis*. Orangevale, CA: Palmer Enterprises.
9. Marilyn B., Peterson, Bob, Morehouse & Richard, Wright (2000). Intelligence 2000: Revising the Basic Elements. Published by Law Enforcement Intelligence Unit (L.E.I.U.) International Association of Law Enforcement Intelligence Analysts (IALEIA).
10. Neil, Quarmby & Lisa Jane, Young (2010). *Managing Intelligence: The Art of Influence*. The Federation Press.

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.