Олександр КОРИСТІН Сергій ДЕМЕДЮК

OSINT

OPEN SOURCE INTELLIGENCE

КНИГА 1

АПАРАТ РАДИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Олександр КОРИСТІН Сергій ДЕМЕДЮК

OSINT
OPEN SOURCE INTELLIGENCE

Теорія та методологія

Видано за підтримки
CRDF Global в Україні

2025

УДК 004.056.5:351.861:351.746.1:343.1

О 73

DOI: 10.32782/osint-theory-2025

Рекомендовано до друку:
вченою радою Одеського державного університету внутрішніх справ
(протокол № 11 від 26 серпня 2025 року)

Рецензенти:

Корченко О. Г. – член-кореспондент НАН України, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, заслужений діяч науки і техніки України;

Корнієнко М.В. – доктор юридичних наук, професор;

Мовчан А.В. – доктор юридичних наук, професор.

OSINT Open Source Intelligence. Теорія та методологія : монографія / Користін О., Демедюк С., Барановський О., Ланде Д. та ін., за заг. ред. Користіна О.Є., Демедюка С.В. – Київ: 7БЦ, 2025. 304 с.
ISBN 978-617-8794-18-7

Монографія "OSINT: теорія та методологія" пропонує цілісну рамку осмислення розвідки з відкритих джерел як стратегічної спроможності держави та як середовища, у якому формується нова логіка реагування на виклики цифрової доби. Видання розкриває роль OSINT у національній безпеці, кіберзахисті, діяльності правоохоронних органів та у громадських ініціативах.

Методологічний блок формує нормативно-етичні та правові засади застосування OSINT: від принципів і процедур до питань територіальної юрисдикції, інтеграції інструментів у наявні інформаційні системи та автоматизації аналітичних процесів за допомогою смартконтрактів. Представлено вітчизняні інновації – семантичний нетворкінг, використання ШІ, інструменти раннього виявлення інформаційних операцій, системи ситуаційної обізнаності та аналіз цифрового сліду.

Практико-правовий вимір зосереджує увагу на застосуванні OSINT у досудовому розслідуванні: судова практика, статус і допустимість електронних доказів, використання даних із Deep Web та Dark Web і пов'язані виклики.

Монографія адресована фахівцям сектору безпеки й оборони, правоохоронцям, правникам, аналітикам, дослідникам, викладачам і здобувачам вищої освіти, які прагнуть системно опанувати теорію й методологію, позиціонуючи Україну активним суб'єктом формування практик, етичних стандартів та технологічних рішень у глобальному просторі OSINT.

УДК 004.056.5:351.861:351.746.1:343.1

ISBN 978-617-8794-18-7

Присвячується правоохоронцям та всім захисникам України — і тим, хто тримає рубіж, і тим, хто тримає лінію даних, перетворюючи відкриті джерела на силу правди та доказ свободи.

Усім, хто стоїть на варті — у полях, у містах і в цифровому просторі: незламним захисникам і дослідникам відкритих джерел, які роблять невидиме видимим заради свободи.

Ця праця — на честь тих, хто боронить державу, і тих, хто збирає крихти відкритих даних у цілісні докази, щоб правда перемагала, а Україна жила вільно.

ЗМІСТ

TABLE OF CONTENTS

ПЕРЕДМОВА

В умовах повномасштабної війни, що триває вже понад три роки, стало очевидним: кіберпростір є повноцінним полем бойових дій. Збройне протистояння доповнюється технологічним і перемога визначається не лише на фронті, а й у цифровому середовищі. Технології в умовах конфлікту розвиваються швидко, особливо в кіберсфері, де нові загрози та тактики з'являються швидше, ніж встигають адаптуватися традиційні системи захисту. Це вимагає постійного оновлення підходів на рівні державних інституцій, відповідальних за національну безпеку.

Агресор веде системну кібервійну, спрямовану на дестабілізацію державного управління, підрив суспільної довіри та руйнування інституційної цілісності. Російські спецслужби та хакерські угруповання здійснюють скоординовані кібератаки, поєднуючи їх з інформаційними впливами. У відповідь Україна має розвивати власну екосистему кіберзахисту, зменшуючи залежність від зовнішніх рішень і зміцнюючи внутрішні аналітичні спроможності.

У цих умовах особливого значення набуває розвиток розвідувально-аналітичних підходів, зокрема – фахової роботи з відкритими джерелами. OSINT дозволяє виявляти загрози на ранніх етапах, підтримувати управлінські рішення та формувати доказову базу. Це не лише інструмент, а складова стратегічного мислення в умовах гібридної війни.

Монографія, підготовлена авторським колективом, є внеском у розвиток національної школи OSINT. Вона системно розглядає Open-Source Intelligence (OSINT) у сучасній моделі правоохоронної діяльності, акцентуючи увагу на методології, термінології, етичних принципах і практичній інтеграції в роботу правоохоронних органів. Важливо, що автори враховують українські правові, професійні та

FOREWORD

In the context of a full-scale war that has lasted for more than three years, it has become clear that cyberspace is a fully-fledged battlefield. Armed confrontation is now complemented by technological warfare, and victory is determined not only on the front lines but also in the digital domain. Technologies evolve rapidly during armed conflicts, especially in the cyber sphere, where new threats and tactics emerge faster than traditional defense systems can adapt. This requires continuous updates to approaches at the level of state institutions responsible for national security.

The aggressor conducts a systematic cyberwar aimed at destabilizing public administration, undermining societal trust, and disrupting institutional integrity. Russian intelligence services and hacker groups carry out coordinated cyberattacks, combining them with information operations. In response, Ukraine must develop its own cybersecurity ecosystem, reduce dependence on external technologies, and strengthen internal analytical capabilities.

Under these conditions, the development of intelligence and analytical approaches becomes particularly important – especially professional work with open sources. OSINT enables early threat detection, supports decision-making, and provides an evidentiary foundation. It is not just a tool, but a component of strategic thinking in hybrid warfare.

The monograph, prepared by a team of authors, contributes to the development of a national OSINT school. It provides a systematic examination of Open-Source Intelligence (OSINT) within the modern model of law enforcement, with a focus on methodology, terminology, ethical principles, and practical integration into the work of law enforcement agencies. Importantly, the authors take into account Ukraine's legal, professional, and resource-specific realities, aligning

ресурсні реалії, поєднуючи міжнародні стандарти з національними потребами.

Це видання не лише про інструменти. Це про здатність бачити загрози до того, як вони стануть фактами, про відповідальність аналітика перед суспільством і про силу знань, що захищають державу.

Формування фахових компетентностей у сфері OSINT – це не лише освітнє чи професійне завдання. Це елемент національної стійкості, що забезпечує здатність діяти проактивно, відповідально й ефективно.

Війна триває. І саме тому ця монографія є на часі.

Сергій Демедюк, доктор філософії в галузі права

заступник секретаря Ради національної безпеки і оборони України

international standards with national needs.

This publication is not only about tools. It is about the ability to identify threats before they materialize, about the analyst's responsibility to society, and about the power of knowledge that protects the state.

Developing professional competencies in OSINT is not just an educational or technical task. It is a component of national resilience that ensures the ability to act proactively, responsibly, and effectively.

The war continues. That is why this monograph is timely.

Serhii Demediuk, PhD

Deputy Secretary National Security and Defense Council of Ukraine

У світі, де інформація стала не лише ресурсом, а й інструментом безпеки, здатність працювати з відкритими даними – це не просто навичка, а стратегічна перевага. Відкриті джерела – це сучасний інтелектуальний простір, у якому формується ситуаційна обізнаність, приймаються рішення, виявляються ризики. Саме тому CRDF Global підтримує розвиток OSINT в Україні – як інструменту національної стійкості, цифрової трансформації та міжнародної інтеграції.

Це двотомне видання – *OSINT: Теорія та методологія і OSINT: Інструменти та методи* – є унікальним внеском у формування системного, багаторівневого підходу до розвідки з відкритих джерел. Його структура охоплює чотири взаємопов'язані домени: стратегічне бачення OSINT як компонента національної безпеки, методологічні основи процесу збору та перевірки даних, інструментальну архітектуру цифрових рішень, а також правові та етичні засади використання відкритої інформації.

У першому томі розглядаються парадигми OSINT у секторі оборони, виклики воєнного часу, інтеграція з кібербезпекою, міжнародні кейси, етичні норми, а також перспективи автоматизації через смарт-контракти. Другий том зосереджений на практичних аспектах: налаштуванні безпечного середовища, роботі з фреймворками, соціальними мережами, цифровими слідами, метаданими, криптоактивами, інструментами Python та штучного інтелекту. Такий підхід дозволяє не лише аналізувати дані, а й будувати повноцінні процеси OSINT-розслідувань, оцінювати ризики, перевіряти контрагентів, документувати воєнні злочини, інтегрувати інструменти у ситуаційні центри та юридичні процедури.

Видання відповідає потребам державних органів, приватного сектору, освітніх установ і громадянського суспільства, формуючи нову культуру роботи з відкритими джерелами – відповідальну, технологічну, правомірну.

CRDF Global в Україні підтримує розвиток

In a world where information has become not only a resource but also a security tool, the ability to work with open data is not just a skill but a strategic advantage. Open sources are a modern intellectual space where situational awareness is formed, decisions are made, and risks are identified. That is why CRDF Global supports the development of OSINT in Ukraine as a tool for national resilience, digital transformation, and international integration.

This two-volume publication – *OSINT: Theory and Methodology and OSINT: Tools and Methods* – is a unique contribution to the formation of a systematic, multi-level approach to open-source intelligence. Its structure covers four interrelated domains: the strategic vision of OSINT as a component of national security, the methodological foundations of the data collection and verification process, the instrumental architecture of digital solutions, and the legal and ethical foundations of open information use.

The first volume examines OSINT paradigms in the defense sector, wartime challenges, integration with cybersecurity, international case studies, ethical standards, and the prospects for automation through smart contracts. The second volume focuses on practical aspects: setting up a secure environment, working with frameworks, social networks, digital traces, metadata, crypto assets, Python tools, and artificial intelligence. This approach allows not only to analyze data, but also to build full-fledged OSINT investigation processes, assess risks, verify counterparties, document war crimes, and integrate tools into situation centers and legal procedures.

The publication meets the needs of government agencies, the private sector, educational institutions, and civil society, shaping a new culture of working with open sources – one that is responsible, technological, and lawful.

CRDF Global in Ukraine supports the development of cybersecurity, digital literacy, and analytical culture. We

кібербезпеки, цифрової грамотності та аналітичної культури. Ми працюємо з державними установами, освітніми закладами, громадськими організаціями, щоб посилити кіберстійкість, впровадити сучасні стандарти, надати доступ до знань і технологій. У межах наших програм ми підтримуємо тренінги, грантові ініціативи, освітні платформи – і саме це видання є прикладом такої синергії.

Особливо важливо, що книга не обмежується технічними аспектами. Вона порушує питання етики, правової допустимості, міжнародної співпраці. Вона готує нову генерацію аналітиків, слідчих, кіберфахівців, які здатні працювати на перетині даних, права і безпеки. Це не просто навчальний посібник – це платформа для формування нової культури роботи з відкритими джерелами.

Ми переконані, що розвиток OSINT в Україні має стратегічне значення. І ми пишаємося тим, що можемо підтримати це видання – як інтелектуальний ресурс, як освітній інструмент, як крок до спільної безпеки.

Михайло ВЕРИЧ

Регіональний директор CRDF Global в Україні

work with government agencies, educational institutions, and non-governmental organizations to strengthen cyber resilience, implement modern standards, and provide access to knowledge and technology. As part of our programs, we support training, grant initiatives, and educational platforms – and this publication is an example of such synergy.

It is particularly important that the book is not limited to technical aspects. It raises issues of ethics, legal admissibility, and international cooperation. It prepares a new generation of analysts, investigators, and cyber experts who are able to work at the intersection of data, law, and security. This is not just a textbook – it is a platform for shaping a new culture of working with open sources.

We are convinced that the development of OSINT in Ukraine is of strategic importance. And we are proud to support this publication – as an intellectual resource, as an educational tool, and as a step toward shared security.

Mykhailo VERYCH

Regional Director, CRDF Global Representation in Ukraine

Висловлення подяки

Апарат Ради національної безпеки і оборони України та Одеський державний університет внутрішніх справ засвідчують глибоку повагу та висловлюють вдячність

Тим, хто тримає небо над Україною.

***Усім захисникам і захисницям**, які щодня виборюють не лише територіальну цілісність держави, а й свободу українського народу, його право на гідність, волю та голос. Саме завдяки вам Україна стоїть, говорить і бореться.*

Тим, хто інвестує в знання і безпеку.

***CRDF Global в Україні** – за багаторічну підтримку процесів розбудови кібербезпеки, за віру в потенціал українських науковців і фахівців, за мотивацію до досліджень і навчання, а також за безпосередню участь у створенні цієї монографії. Ваш внесок – це не просто підтримка, це стратегічне партнерство, що формує інтелектуальний щит держави.*

Тим, хто будує мости знань крізь кордони.

Нашим зарубіжним партнерам і колегам

Michael Bazzell – американський експерт з OSINT, колишній співробітник ФБР, автор низки впливових посібників з цифрової розвідки та приватності, засновник платформи IntelTechniques;

Dr Christopher Ahlberg – шведсько-американський науковець, член Шведської королівської академії інженерних наук, співзасновник і генеральний директор компанії Recorded Future, яка зараз входить до складу Mastercard;

за плідну співпрацю, неоціненні фахові поради та щедро надану професійну літературу. Ваш внесок – це не просто підтримка, це інтелектуальний обмін, що зміцнює українську експертизу, розширює горизонти і формує спільну мову безпеки, права та науки.

Тим, хто тримає дзеркало перед текстом.

Рецензентам

Олександр КОРЧЕНКО – член-кореспондент НАН України, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, заслужений діяч науки і техніки України;

Максим КОРНІЄНКО – доктор юридичних наук, професор;

Анатолій МОВЧАН – доктор юридичних наук, професор;

за проявлений інтерес до нашої роботи, за відверті відгуки, слушні зауваження та цінні поради, які стали каталізатором змістовного вдосконалення. Ваш критичний погляд – це не просто оцінка, це співавторство в пошуку точності, логіки та глибини.

Тим, хто перетворює ідею на спільну справу.

керівникам проєкту

Олександр КОРИСТІН – доктор юридичних наук, професор, заслужений діяч науки і техніки України – Департамент кіберполіції НПУ; Інститут дослідження кібервійни;

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

за ініціативу, що стала основою цієї роботи, за вміння об'єднати найкращих фахівців у спільноту знань і дії, за редакційне бачення, яке надало змісту логіку, а тексту – силу. Лідерство – це не лише організація, це архітектура довіри, професіоналізму та спільної відповідальності.

Подяка тим, хто перетворює знання на інструмент дії. Висловлюємо глибоку вдячність ***авторському колективу*** – видатним науковцям, практикам, експертам у сфері безпеки, поліцейської роботи, OSINT та креативного аналітичного мислення – за змістовний внесок у дослідження, розробку монографії та навчального посібника, а також за підготовку окремих розділів цього видання. Саме завдяки вашій синергії теорія набуває практичного звучання, а кожна сторінка – стратегічної ваги.

Дмитро АФОНІН – кандидат юридичних наук, доцент – *Національний університет «Одеська юридична академія»;*

Олексій БАРАНОВСЬКИЙ – кандидат технічних наук, CISM, CISSP – *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»; департамент комп'ютерних наук Технічного інституту Блекінге (Швеція);*

Михайло ВЕРИЧ – регіональний директор CRDF Global в Україні;

Анатолій ВОЙТКО – Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», інженер даних LetsData;

Людмила ГАВРИЛЮК – кандидат юридичних наук, старший дослідник – *Національна академія внутрішніх справ;*

Юрій КАРДАШЕВСЬКИЙ – доктор філософії права – *Національне агентство з питань запобігання корупції;*

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

Дмитро ЛАНДЕ – доктор технічних наук, професор, Лауреат Премії Кабінету Міністрів України, Лауреат Премії НАН України імені В. М. Глушкова – *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»; Інститут проблем реєстрації інформації НАН України;*

Володимир ЛОЗОВИЙ – ТОВ «АРТЕЛЛЕНС УКРАЇНА»

Роман ОСАДЧУК – Національний університет «Києво-Могилянська академія»; директор з розвідки загроз LetsData;

Денис ПЕФТІЄВ – керівник Управління кримінального аналізу НПУ у 2018-2020 рр.; засновник "IDiAnalytics";

Сергій ПРОКОПЕНКО – управління забезпечення діяльності НКЦК служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України;

Анатолій ПЯСЕЦЬКИЙ – ТОВ «Ю-КОНТРОЛ»;

Роман РАСКЕВИЧ – Державна прикордонна служба України;

Наталія СВИРИДЮК – доктор юридичних наук, професор – *Одеський державний університет внутрішніх справ;*

Дмитро ХУДЕНКО – ветеран Національної поліції України; керівник Департаменту кримінального аналізу НПУ у 2021-2023 рр.;

Наталія ЦЮПРИК – кандидат юридичних наук – *Національна академія внутрішніх справ;*

Елліна ШНУРКО-ТАБАКОВА – ГО «Рада інформаційної безпеки та кіберзахисту»; Інформаційно-аналітичний сервіс Атак Індекс.

"Той, хто не бореться за контроль над даними, рано чи пізно втратить контроль над реальністю" –

Авторська формула

ВСТУП

Передумови та обґрунтування

Становлення незалежної та стійкої Української держави нерозривно пов'язане з розбудовою всеохоплюючої системи національної безпеки, спроможної ефективно реагувати на гібридні загрози та воєнні виклики. Сучасні безпекові умови, зумовлені збройною агресією проти України, трансформацією технологічного середовища та глобалізацією інформаційних процесів, формують нову парадигму захисту державних і суспільних інтересів.

У центрі цієї парадигми – переорієнтація правоохоронної діяльності з реактивної моделі на **проактивну, аналітично керовану стратегію**, що інтегрує принципи *Intelligence-led Policing* та можливості відкритої розвідки (*Open-Source Intelligence – OSINT*).

OSINT виступає як багатофункціональний інструмент, здатний не лише ідентифікувати та прогнозувати криміногенні процеси, але й забезпечувати стратегічну підтримку ухвалення управлінських рішень. Його потенціал у поєднанні з методологіями оцінювання ризиків та виявлення вразливостей дозволяє створювати адаптивну, стійку й етично вивірену аналітичну екосистему.

Впровадження OSINT у національну практику вимагає глибокого методологічного обґрунтування, інтеграції міжнародних стандартів і водночас врахування українських реалій. Саме цим завданням і присвячено цю монографію – з метою не лише опису інструментарію, а й формування цілісної концептуальної рамки для його сталого використання у системі національної безпеки.

Background and rationale

The establishment of an independent and resilient Ukrainian state is inextricably linked to the development of a comprehensive national security system capable of effectively responding to hybrid threats and military challenges. The current security environment – shaped by armed aggression against Ukraine, the transformation of the technological landscape, and the globalization of information processes – defines a new paradigm for protecting national and societal interests.

At the core of this paradigm lies a shift in law enforcement from a reactive model to **a proactive, analytically driven strategy** that integrates the principles of Intelligence-led Policing and the capabilities of Open-Source Intelligence (OSINT).

OSINT serves as a multifunctional tool, capable not only of identifying and forecasting criminogenic processes but also of providing strategic support for decision-making. Its potential, combined with methodologies for risk assessment and vulnerability detection, enables the creation of an adaptive, resilient and ethically grounded analytical ecosystem.

The implementation of OSINT in national practice requires deep methodological justification, integration of international standards, and careful consideration of Ukrainian realities. This monograph is dedicated to that very task – not merely to describe the tools, but to establish a coherent conceptual framework for their sustainable application within the national security system.

Мета та особлива роль

Ця монографія покликана здійснити системне наукове осмислення ролі розвідки з відкритих джерел (OSINT) як ключового складника сучасної моделі правоохоронної діяльності, керованої аналітичною розвідкою (Intelligence-led Policing, ILP), і сформувати методологічний фундамент її адаптації до українських умов. У фокусі дослідження – не лише технічні можливості збору інформації з відкритих джерел, а й побудова OSINT як зрілої аналітичної дисципліни, інтегрованої в багаторівневу систему аналізу та стратегічного управління безпекою.

OSINT розглядається комплексно: через призму уніфікованої термінології, узгодженої з міжнародними стандартами, але вкоріненої в українську правову і професійну традицію; через критичне осмислення різночитань англомовних дефініцій та уникнення кальок, які спотворюють сутність поняття; через зіставлення зарубіжних концептуальних моделей та вітчизняних реалій безпекового середовища.

Особлива роль цього видання полягає у виконанні функції методологічного мосту між світовими напрацюваннями у сфері розвідки з відкритих джерел та потребами українських інституцій, що діють в умовах воєнної агресії, гібридних загроз і обмежених ресурсів. Монографія пропонує системну рамку для впровадження OSINT у структуру ILP – від визначення місця цієї розвідки в загальній архітектурі аналізу, до формування алгоритмів взаємодії між різними суб'єктами сектору безпеки, оборони та громадянського суспільства.

Вона орієнтована на розробників державної політики, керівників правоохоронних і спеціальних підрозділів, науковців та практиків, які прагнуть не лише запозичувати методики, а й творити власну школу OSINT в Україні. Цей науковий доробок спрямований на інституційне закріплення відкритої розвідки як інструмента стратегічного мислення, прогнозування та випереджального реагування, що забезпечує професійну

Objective and added value

This monograph is intended to provide a systematic scholarly reflection on the role of Open-Source Intelligence (OSINT) as a key component of the modern model of law enforcement guided by Intelligence-led Policing (ILP), and to establish a methodological foundation for its adaptation to Ukrainian conditions. The focus of the study extends beyond the technical capabilities of collecting information from open sources to the construction of OSINT as a mature analytical discipline, integrated into a multi-level system of analysis and strategic security management.

OSINT is examined comprehensively: through the lens of unified terminology aligned with international standards yet rooted in Ukrainian legal and professional tradition; through critical reflection on the divergent interpretations of English-language definitions and the avoidance of literal translations that distort the essence of the concept; and through the comparison of foreign conceptual models with domestic security realities.

The distinctive role of this publication lies in its function as a methodological bridge between global developments in open-source intelligence and the needs of Ukrainian institutions operating under conditions of military aggression, hybrid threats, and limited resources. The monograph offers a systemic framework for integrating OSINT into the ILP structure – from defining its place within the overall architecture of analysis to developing interaction algorithms among various actors in the security, defense and civil society sectors.

It is intended for policymakers, heads of law enforcement and special units, scholars, and practitioners who seek not only to adopt methodologies but also to build a Ukrainian school of OSINT. This scholarly contribution aims to institutionalize open-source intelligence as a tool of strategic thinking, forecasting, and anticipatory

доброчесність, доказову силу та міжнародну сумісність дій українських аналітиків.

response – ensuring professional integrity, evidentiary strength, and international interoperability in the actions of Ukrainian analysts.

Олександр КОРИСТІН
доктор юридичних наук, професор

Oleksandr KORYSTIN
DSc Law, Professor

"Коли дані стають доступними, а технології – прозорими, безпека перестає бути привілеєм і стає правом"

Авторська формула, умотивована ідеями Карла Сагана, Юваля Ноя Харарі, Едварда Сноудена та Лоуренса Лессіга

ПАРАДИГМА OSINT В СЕКТОРІ БЕЗПЕКИ І ОБОРОНИ

ЧАСТИНА І

РОЗДІЛ 1

СТРАТЕГІЧНИЙ ЛАНДШАФТ ЗАСТОСУВАННЯ OSINT В СЕКТОРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Сергій ДЕМЕДЮК

Першочерговим обов'язком держави залишається забезпечення безпеки її громадян. Спектр загроз національній безпеці стає все більш складним та різноманітним. Тероризм, кібератаки, нетрадиційні атаки із застосуванням хімічної, ядерної або біологічної зброї, а також масштабні аварії або природні катаклізми – будь-що може поставити під загрозу безпеку громадян, завдавши серйозної шкоди інтересам та економічному добробуту країни. В умовах економічної невизначеності та політичної нестабільності уряди повинні бути здатними швидко і ефективно реагувати на нові та еволюціонуючі загрози своїй безпеці. Необхідні жорсткі заходи безпеки, щоб захистити громадян, громади та комерцію від сучасних загроз, найактуальнішою з яких залишається постійна загроза міжнародного тероризму.

Незважаючи на те, що Інтернет і соціальні мережі позитивно збагатили суспільні комунікації та економічні можливості, ці технологічні досягнення змінили – і продовжують змінювати – саму природу злочинності, сприяючи появі нових витончених і технічно оснащених злочинців. Крім того, безмежний характер явища кіберзлочинності та транснаціональний характер торгівлі людьми, імпорту наркотиків, незаконного переміщення вогнепальної зброї, готівки та крадених товарів означає, що злочинці можуть планувати свої злочини, перебуваючи в будь-якій точці світу, що робить правоохоронну діяльність особливо складною, і саме тому правоохоронні органи повинні максимально використовувати потенціал OSINT та шукати нові й інноваційні способи запобігання злочинам. Таким чином, для всіх практиків, політиків і правоохоронців важливо розуміти, що таке OSINT і чим він не є, як його можна використовувати, які існують обмеження або умови для цього, а також краще розуміти масштаб, обсяг і складність загроз з боку злочинців, чиї методи роботи стають все більш витонченими.

Щоб ефективно протистояти різноманітним сучасним загрозам безпеці, правоохоронні органи використовують дедалі більше джерел розвідданих, зібраних із загальнодоступної інформації. Невпинне прагнення поліцейських до отримання розвідувальних даних для забезпечення безпеки суспільства за допомогою відкритих джерел інформації призвело до появи найбільш швидкозростаючого поліцейського напряму 21-го сторіччя – напряму, який додає значної цінності та підвищує ефективність боротьби з сучасною злочинністю, що отримав назву *«Розвідка з відкритих джерел»* (OSINT).

Ще до появи сучасних технологічних засобів збору інформації правоохоронні органи планували, готували, збирали та продукували розвідувальні дані з загальнодоступної інформації та відкритих джерел для отримання знань і розуміння, необхідних для запобігання злочинам та переслідування злочинців. Хоча традиційні загрози, пов'язані зі злочинністю, історично виникали на місцевому рівні, в сучасному світі, який стає все більш взаємопов'язаним і взаємозалежним, багато нових небезпек мають транскордонний, транснаціональний вимір, посилюючись завдяки Інтернету, соціальним мережам і більш досконалим мобільним комунікаціям. Соціальні і технічні інновації зараз відбуваються з постійно зростаючою швидкістю, викликаючи швидкі і радикальні зміни в суспільстві. Ці зміни, зумовлені можливостями, пропонованими новими і новітніми технологіями, впливають на громадян, їхні громади, приватний сектор, уряд і, звичайно ж, на поліцію.

Роль правоохоронних органів полягає у підтримці правопорядку, захисті громадян, запобіганні, виявленні та розслідуванні злочинів. Досягаючи цих цілей, правоохоронні органи виконують завдання щодо безпеки суспільства та громадян, яким вони служать. OSINT потенційно може надати правоохоронним органам і органам безпеки критично важливий потенціал для доповнення та посилення їхніх розвідувальних спроможностей. Цілеспрямований і законний моніторинг, аналіз і візуалізація публічних відкритих джерел даних повинні розглядатися як обов'язкові вимоги будь-якої стратегії національної безпеки. Здатність швидко збирати, точно обробляти та аналізувати дані з відкритих джерел може стати значною допомогою під час розслідувань, а також використовуватися для стратегічного планування боротьби зі злочинністю на національному рівні. Однак для досягнення ефективних та інноваційних рішень, правоохоронним органам доцільно розглянути можливість співпраці з приватними та державними партнерами, включаючи наукові кола.

ТЕРОРИЗМ ТА ПРОПОРЦІЙНІСТЬ OSINT ВІДПОВІДІ

Терористичні загрози є предметом серйозного громадського та політичного занепокоєння, але вони також ставлять гострі виклики перед державним апаратом безпеки. Ці виклики виникають тому, що тероризм може спричинити значні людські жертви, але не масштаби звірств, скоєних в його ім'я, надають тероризму особливого статусу, а загроза, яку він становить для держави, оскільки він підриває основу державної легітимності – здатність захищати своїх громадян. Тому заходи, відомі як боротьба з тероризмом, як один з основних аспектів національної безпеки, привертають велику політичну і громадську увагу, і, відповідно, невдачі в боротьбі з тероризмом призводять до значного резонансу, за яким слідує суворий контроль з боку різних сторін, включаючи засоби масової інформації, громадську думку, поліцейські розслідування, урядові розслідування, парламентські запити і академічні дослідження.

З огляду на масштаб і складність загроз міжнародного тероризму, спецслужби повинні продовжувати вдосконалювати антитерористичні заходи, щоб убезпечити нас усіх; і, що найважливіше, шукати нові шляхи впровадження прогресивних розробок, щоб гарантувати, що основним рушієм змін у практиці боротьби з тероризмом є не просто наступна успішна атака. Використання можливостей OSINT за допомогою великих даних продовжує змінювати правила гри для політиків, фахівців і практиків у сфері боротьби з тероризмом.

Протягом останніх десяти-п'ятнадцяти років OSINT все частіше використовується організаціями приватного сектору як засіб вимірювання лояльності клієнтів, відстеження громадської думки та оцінки сприйняття продукції. Аналогічно, правоохоронні органи та органи безпеки визнають необхідність застосування подібних методів для посилення своїх слідчих можливостей та покращення здатності виявляти й реагувати на кримінальні загрози. Кримінальні суб'єкти, що продукують ці загрози, використовують Інтернет для вербування, створення незаконних картелів та передачі інформації і грошей для фінансування і координації своєї незаконної діяльності.

Поширення Інтернету переплело континенти, культури і спільноти, а також інтегрувало його з більшістю сучасних технологій. Хоча соціальні медіа залишаються домінуючою онлайн-платформою для кримінальних та екстремістських психологічних операцій, існує все більший потенціал для того, щоб піти шляхом інтернету, розгалужуючись, використовуючи ігрові консолі[1], мобільні додатки[2], хмарні сховища[3] і P2P-сервіси. У той час як

[1] Tassi, P. (2015). "How ISIS terrorists may have used PlayStation 4 to discuss and plan attacks". Forbes Online. http://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis-terrorists-used-ps4-to-plan-attacks/#39d5c755731a

[2] Billington, J. (2015). "Paris terrorists used WhatsApp and Telegram to plot attacks according to investigators". International Business Times. http://www.ibtimes.co.uk/paris-terrorists-used-whatsapp-telegram-plot-attacks-according-investigators-1533880

[3] Hall, K. (2011). "Cyber terrorism set to increase after al-Qaeda calls for more cyber-attacks, says government". Computer Weekly Online. http://www.computerweekly.com/news/2240105012/Cyber-terrorism-set-to-increase-after-al-Qaeda-calls-for-more-cyber-attacks-says-government

і результативно для досягнення спільного ефекту від їхніх колективних зусиль, невидимі наслідки або каскадні ефекти, що виникають через взаємозалежність самої системи, означають, що погано обґрунтоване прийняття рішень може призвести до втрат життів, а також до економічних витрат, фізичної шкоди або суспільного добробуту. OSINT є зростаючим і все більш важливим аспектом у прийнятті рішень правоохоронними органами в таких ситуаціях – і це було ще до того, як зростаюче використання соціальних мереж вивело на перший план відкритий код. Поява соціальних мереж як джерела розвідувальної інформації з відкритих джерел здебільшого призвела до розширення обсягу і спектру джерел OSINT, які тепер доступні для більшого кола аудиторії, користувачів і додатків. По суті, якщо система, в якій вона знаходиться і використовується, в даному випадку розвідувальний цикл, не є такою ж інтероперабельною, як і система, в якій відбувається прийняття рішень, то застосування і цінність OSINT буде набагато менш ефективною, дієвою і значущою.

Один з прикладів, який надає корисний історичний контекст для розвитку і використання цього виду діяльності, наведено в тематичному дослідженні 2002 року в Австралії, задокументованому в звіті НАТО про OSINT[25] (NATO 2002).

ВИСНОВКИ

Світ переосмислюється завдяки відкритим джерелам. Загальнодоступна інформація може бути використана різними особами та організаціями для досягнення широкого спектру цілей, і правоохоронні органи все частіше ефективно використовують це безкоштовне та доступне джерело інформації. Хоча Інтернет та соціальні мережі позитивно збагатили суспільні комунікації та економічні можливості, ці технологічні досягнення змінили – і продовжують змінювати – саму природу злочинності, сприяючи появі нових витончених і технічно оснащених злочинців. Характер деяких *«традиційних»* видів злочинів трансформувався завдяки використанню комп'ютерів та інформаційно-комунікаційних технологій (ІКТ) з точки зору їхнього масштабу та охоплення, а загрози та ризики поширилися на багато аспектів суспільного життя. Також з'явилися нові форми злочинної діяльності, спрямовані на порушення цілісності комп'ютерів і комп'ютерних мереж. Загрози існують не лише для окремих осіб і бізнесу, але й для національної безпеки та інфраструктури.

Крім того, безмежний характер явища кіберзлочинності та транснаціональний характер торгівлі людьми, імпорту наркотиків і незаконного переміщення вогнепальної зброї, готівки та крадених товарів означає, що злочинці можуть планувати свої злочини з юрисдикцій по всьому світу, що робить правоохоронну діяльність особливо складною, і саме тому правоохоронні органи повинні максимально використовувати потенціал OSINT та шукати нові інноваційні способи запобігання злочинам. Прогресивні та далекоглядні правоохоронні органи, які заохочують, приймають та використовують можливості OSINT, будуть краще підготовлені до майбутніх викликів у сфері безпеки, і, як наслідок, матимуть більше можливостей для забезпечення безпеки громад, яким вони служать, а також для того, щоб вони почували себе в більшій безпеці.

Здатність правоохоронних органів використовувати можливості OSINT буде дедалі більше відрізнятися – розмежування між тими поліцейськими силами, які є лідерами, і тими, які просто слідують за ними. Тому прийняття правової та етичної бази для ефективного використання OSINT є вкрай необхідним не лише для того, щоб реалізувати переваги можливостей OSINT для запобігання злочинам, переслідування злочинців та підготовки до нових викликів і загроз, але й для підвищення ефективності та результативності послуг, які надають правоохоронні органи, а також для кращого захисту публічної інформації, якою вони користуються. Але поки OSINT залишається значною мірою

[25] NATO (2002) NATO open source intelligence reader.
http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/ NATOOSINTReaderFINAL11OCT02.pdf

неврегульованим серед правоохоронних органів, і жодна установа не має права власності або першості, непотрібне дублювання доступу та небажані посягання на конфіденційність даних громадян, ймовірно, будуть постійною особливістю зростаючого використання OSINT в майбутньому. Тому правоохоронні органи ніколи не повинні забувати, що неналежний доступ і використання OSINT лише посилює аргументацію на користь запровадження жорстких інструкцій, посилення законів і загалом обмеження вільного доступу до публічної інформації та її збору. Крім того, правоохоронним органам слід забезпечити, щоб використання всіх OSINT відповідало формальним процесам моделі управління розвідкою. Такий підхід дозволить зберегти і зміцнити довіру громад, яким вони служать, у тому, що доступ до їхньої загальнодоступної інформації здійснюється на законних підставах з метою боротьби зі злочинністю та забезпечення безпеки співгромадян.

Інформація з відкритих джерел отримується з газет, журналів, радіо, телебачення та Інтернету. Аналітики вже давно використовують таку інформацію як доповнення до засекречених даних, але систематичний збір інформації з відкритих джерел не був пріоритетом розвідувального співтовариства. Останніми роками, з огляду на зміни в міжнародному середовищі, особливо після подій 11 вересня, лунають заклики до більш інтенсивного і цілеспрямованого інвестування в збір і аналіз інформації з відкритих джерел. Однак дехто все ще наголошує на тому, що основним завданням розвідки залишається отримання і аналіз таємного контенту.

Зараз існує консенсус щодо того, що OSINT необхідно систематично здійснювати і він має стати важливим компонентом аналітичних процесів. Це було визнано різними комісіями і закріплено в законах. Загалом, зазначається про цінність використання OSINT в усіх аспектах повсякденної діяльності правоохоронних органів. Однак, ще не так давно, у 2016 році, не використовувалися терміни «соціальні медіа», «супутник» і «дрони», які експоненціально розвиваються, здешевлюються і використовуються все ширше. Таке зростання призвело до того, що під час холодної війни на OSINT припадало лише 10 % інформаційного забезпечення розвідки, а 90 % походило з закритих джерел. Сьогодні ситуація змінилася, і 90 % інформації і даних для розвідки надходить від OSINT.

Експоненціальне зростання доступності OSINT і його використання правоохоронними органами зумовлює необхідність забезпечення повної інтеграції OSINT, як він існує зараз і може розвиватися в майбутньому, з розвідувальними даними із закритих джерел; і все це в рамках загальної системи управління інформацією. Таким чином, можна досягти більш точного, своєчасного та належного використання інформації в повсякденному процесі прийняття рішень.

Дуже важливо, що це забезпечило б вищий рівень впевненості у використанні таких розвідувальних даних, оскільки обидва джерела надають взаємну підтримку, щоб запевнити як правоохоронні органи, так і громадян, яким вони служать, у тому, що рішення, які вони приймають, ґрунтуються на найбільш надійній, точній і достовірній інформації, доступній на той час, і що в результаті приймаються більш обґрунтовані рішення. Досягнення такого результату могло б зменшити ймовірну шкоду для політичної та розвідувальної спільнот.

РОЗДІЛ 2

ІНФОРМАЦІЙНА РОЗВІДКА З ВІДКРИТИХ ДЖЕРЕЛ: ВИКЛИКИ, РИЗИКИ ТА ПОТЕНЦІАЛ У ВОЄННИЙ ЧАС

Наталія СВИРИДЮК
Дмитро АФОНІН

Наше сьогодення характеризується стрімким розвитком цифрових технологій, які суттєво трансформували як природу сучасних міжнародних конфліктів, так і характер загроз національній та міжнародній безпеці. Зростання відкритості суспільств, розширення доступу до інформаційних ресурсів, а також глобалізація обміну даними зумовили формування нової аналітичної парадигми, у межах якої відкриті джерела інформації набули виняткового значення. Водночас цифровізація суспільства радикально змінила підходи до ведення воєнних конфліктів і зумовила появу нових засобів інформаційного впливу. У цьому контексті особливого значення набуває OSINT (Open Source Intelligence – розвідка з відкритих джерел), який став вагомим інструментом не лише у військово-стратегічному вимірі, але й у політичному, соціальному та правовому контекстах. В умовах зростання гібридних загроз та інтенсивного інформаційного протистояння OSINT поступово перетворюється на критичний компонент безпекової стратегії[1].

OSINT охоплює процес збору, аналізу та інтерпретації інформації з відкритих джерел, що не потребує спеціального доступу чи технічних засобів збору розвідувальних даних (наприклад, прослуховування або перехоплення)[2]. Йдеться про такі відкриті джерела, як офіційні вебсайти, соціальні мережі, форуми, медіаплатформи, бази даних, наукові публікації, державні реєстри, супутникові знімки тощо[3]. На відміну від традиційних форм розвідки таких як HUMINT (агентурна розвідка) чи SIGINT (технічна розвідка), OSINT базується на публічно доступній інформації, що дозволяє використовувати її не лише органами державної влади, а й відкриває можливість використання зазначеного інструменту й широкому колу осіб: представникам громадянського суспільства, науковцям, дослідникам, журналістам, правоохоронним структурам, військовим, волонтерам і навіть приватним особам.

Під час повномасштабного вторгнення росії в Україну у 2022 році значущість та роль OSINT значно зросла. Розвідка з відкритих джерел дозволила оперативно верифікувати атаки, документувати воєнні злочини, фіксувати переміщення військових підрозділів, ідентифікувати логістичні маршрути, а також OSINT забезпечує можливість отримання оперативних даних щодо морально-психологічного стану цивільного населення та військовослужбовців, рівня інфраструктурних втрат, актуальних гуманітарних потреб тощо. У багатьох випадках інформація з відкритих джерел забезпечувала точнішу картину, ніж традиційні розвідувальні методи, завдяки швидкості її поширення та колективному аналізу.

При цьому OSINT не вимагає суттєвих фінансових витрат або застосування високотехнологічних засобів, а базується переважно на аналітичних навичках і здібностях, критичному мисленні та системному підході аналітика. Зокрема, у ході війни в Україні OSINT став ефективним інструментом численних виявлень воєнних злочинів та дезінформаційних кампаній, фіксації наслідків ракетних атак тощо.

---

[1] Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux; Zegart, A. (2022). Spies, Lies, and Algorithms: The History and Future of American Intelligence. Princeton University Press.

[2] Steele, R.D. (2007). Chapter: Open Source Intelligence. In: Loch Johnson (Ed.), Handbook of Intelligence Studies. Routledge.

[3] Open-Source Intelligence & its Legal and Ethical Aspects (July 25, 2024).
URL: https://eithos.eu/open-source-intelligence-osint-its-legal-and-ethical-aspects

правова підтримка волонтерських ініціатив, у тому числі через фонди безпеки, проєкти технічної допомоги, гранти.

Таким чином, інституційна спроможність України у сфері OSINT продовжує розвиватися на тлі війни як результат мобілізації наявних ресурсів, творчої адаптації до викликів та відкритості до партнерств. Проте для переходу до системного управління необхідно інтегрувати зусилля на стратегічному, правовому та кадровому рівнях.

ВИСНОВОК

У сучасних умовах збройної агресії проти України відкриті джерела інформації набули принципово нового значення як в аспекті національної безпеки, так і в контексті інформаційного суверенітету. OSINT, що раніше розглядався як допоміжний аналітичний інструмент, трансформувався у самостійну розвідувальну дисципліну, спроможну не лише доповнювати традиційні форми розвідки, а й забезпечувати критичну підтримку процесів стратегічного планування, документування воєнних злочинів, протидії дезінформації та інформаційного впливу противника.

Під час повномасштабної війни роль OSINT значно зросла – завдяки швидкому доступу до відкритих даних, можливості геолокаційного аналізу, верифікації відео та фото, синтезу соціомедійного контенту, OSINT забезпечує оперативну обізнаність щодо подій на фронті та в тилу. При цьому демократичний характер OSINT, що дозволяє його використання як державними органами, так і волонтерами, журналістами, дослідниками, створює потужний горизонтальний ресурс національного спротиву.

Водночас із перевагами, стрімке поширення OSINT породжує низку серйозних викликів: витоки критичної інформації, свідоме або несвідоме розкриття дислокацій військових підрозділів, логістичних маршрутів, персональних даних, підвищують вразливість країни до кібератак, фізичних диверсій та інформаційно-психологічних операцій. Відсутність належного регламентування використання OSINT, дефіцит цифрової гігієни серед населення, етичні та правові колізії – все це створює ризики як для державної, так і для індивідуальної безпеки.

В умовах воєнного стану нагальною є потреба у створенні цілісної системи управління та захисту процесів розвідки з відкритих джерел. Вона має включати правове врегулювання обігу відкритих даних, розвиток інституційної спроможності аналітичних підрозділів, підвищення рівня інформаційної гігієни та формування культури відповідального ставлення до інформації серед населення. Не менш важливими залишаються питання міжвідомчої взаємодії, технологічної модернізації та поглиблення міжнародної співпраці.

Український досвід переконливо свідчить: для ефективного застосування OSINT необхідний перехід від фрагментарного до системного підходу, який передбачає розробку стратегії державної політики у сфері розвідки з відкритих джерел, визначення чітких меж її правового статусу, створення спеціалізованих платформ і мультидисциплінарних команд.

Особливої уваги потребує формування етичної культури поводження з відкритою інформацією: навіть доступні дані можуть становити загрозу, якщо вони неконтрольовано публікуються або аналізуються без урахування безпекового контексту. Відтак, OSINT повинен розвиватися як інструмент з високим рівнем професіоналізму, стандартизації та міжвідомчої координації.

Таким чином, OSINT – це не лише технологія чи аналітичний інструмент. Це – складова цифрової безпеки, елемент гібридного опору, основа для сучасної моделі безпекового мислення. Його ефективне використання потребує балансу між відкритістю інформації та безпекою, що є основою стійкості держави

у сучасних умовах. Разом з тим, продуктивне застосування OSINT можливе лише за умови поєднання правових гарантій, освітніх зусиль, технологічної спроможності та стратегічного бачення держави. Досвід України показав, що розвідка з відкритих джерел здатна забезпечити оперативність, точність та масштабність аналізу, доповнюючи традиційні методи розвідки. Досвід України у цьому напрямі є унікальним і може стати основою для формування новітніх стандартів розвідки у XXI сторіччі.

РОЗДІЛ 3

OSINT ТА КІБЕРБЕЗПЕКА: ІНТЕГРАЦІЯ ДАНИХ, ТЕХНОЛОГІЙ І РІШЕНЬ

Сергій ПРОКОПЕНКО

Вплив кіберзлочинності змусив розвідувальні та правоохоронні органи по всьому світу боротися з кіберзагрозами. Перед усіма секторами зараз стоять схожі дилеми: як найкраще захиститися від кіберзлочинності і як ефективно сприяти безпеці людей і організацій. Отримання унікальних і цінних розвідувальних даних шляхом збору публічних записів для створення всебічного профілю певних цілей швидко стає важливим засобом для спільноти розвідників. Оскільки кількість доступних відкритих джерел стрімко зростає, протидія кіберзлочинності все більше залежить від передових програмних засобів і методів збору та обробки інформації в ефективний і результативний спосіб.

У XXI сторіччі цифровий світ став *«палицею з двома кінцями»*[1]. Завдяки революції загальнодоступних джерел (тобто відкритих джерел) цифровий світ надав сучасному суспільству величезні переваги, в той же час питання інформаційної незахищеності висвітлили вразливості та слабкості[2]. Спільна інфраструктура Інтернету створює потенціал для взаємопов'язаних вразливостей для всіх користувачів[3]: *«Віруси, хакери, витік безпечної і приватної інформації, системні збої і переривання послуг»* з'явилися в бездонному потоці[4].

У фахових публікаціях зазначають[5], що кіберпростір має чотири унікальні особливості, які називаються *«трансформаційними ключами»*, які дозволяють злочинцям вчиняти злочини:

1. *глобалізація, яка надає злочинцям нові можливості для виходу за межі звичайних кордонів;*
2. *розподілені мережі, які створюють нові можливості для віктимізації;*
3. *синоптизм і панoптизм, які дають можливість стежити за жертвами віддалено;*
4. *сліди даних, які можуть надати злочинцям нові можливості для вчинення крадіжки особистих даних.*

[1] Yuan T, Chen P (2012) Data mining applications in E-Government information security, 2012 international workshop on information and electronics engineering (IWIEE). Proc Eng 29:235– 240

[2] Hobbs Ch, Morgan M, Salisbury D (2014) Open source intelligence in the twenty-first century. Palgrave, pp. 1–6.

[3] Appel EJ (2011) Behavior and technology, Internet Searches for Vetting, Investigations, and Open-Source Intelligence. Taylor and Fransic Group, pp. 3–17.

[4] Yuan T, Chen P (2012) Data mining applications in E-Government information security, 2012 international workshop on information and electronics engineering (IWIEE). Proc Eng 29:235– 240

[5] Wall DS (2008) Hunting shooting, and phishing: new cybercrime challenges for cyber canadians in the 21st Century. The Eccles Centre for American Studies. www.bl.uk/ecclescentre. The British Library Publication; Wall DS (2005) The internet as a conduit for criminal activity. In: Pattavina A (ed) Information technology and the criminal justice system. Sage Publications, USA; Nykodym N, Taylor R, Vilela J (2005) Criminal profiling and insider cyber crime. Digital Invest 2:261–267. Elsevier

На додаток до вищесказаного, стверджується[6] також, що однією з основних тенденцій розвитку Інтернету останніх років є те, що *«підключення до Інтернету може бути дуже ризикованою справою»*.

Окрім епідемічного використання та розвитку технологій мобільного зв'язку, використання відкритих джерел поширюється у сферах розвідки, політики та бізнесу[7]. У той час як традиційні джерела та інформаційні канали (ЗМІ, бази даних, енциклопедії тощо) були змушені адаптуватися до нового віртуального простору, щоб зберегти свою присутність, багато «нових» медіа-джерел (особливо з соціальних мереж) поширюють велику кількість користувацького контенту, який згодом змінив інформаційний ландшафт. Прикладами масштабу інформації, створеної користувачами, є 500 мільйонів твітів на день у Твіттері та 98 мільйонів щоденних записів у блогах на **Tumblr**[8], а також мільйони індивідуальних персональних сторінок у Фейсбуці. З розвитком інформаційного ландшафту правоохоронним органам необхідно збирати відповідний контент за допомогою розслідувань і регульованого спостереження, щоб запобігати і виявляти терористичну діяльність. Кількість даних, інформації збільшується кардинально щоденно.

Загалом, термін *«розвідка з відкритих джерел»* (OSINT) походить від служб національної безпеки та правоохоронних органів[9]. Для наших цілей тут OSINT переважно визначається як *«сканування, пошук, збір, вилучення, використання, перевірка, аналіз і обмін розвідувальною інформацією зі споживачами відкритих джерел і загальнодоступних даних з несекретних, нетаємних джерел»*[10]. OSINT охоплює різні публічні джерела, такі як академічні публікації (наукові роботи, публікації конференцій тощо), джерела ЗМІ (газети, радіоканали, телебачення тощо), веб-контент (веб-сайти, соціальні мережі тощо) та публічні дані (відкриті урядові документи, оголошення публічних компаній тощо)[11].

OSINT традиційно описується як пошук загальнодоступних опублікованих джерел[12], таких як книги, журнали, газети, брошури, звіти тощо. Це часто називають літературною розвідкою або LITINT[13].

Однак, швидке зростання цифрових медіа-джерел в Інтернеті та суспільному мовленні розширило сферу діяльності з відкритими джерелами[14]. Оскільки існують різноманітні публічні онлайн джерела, з яких ми можемо збирати розвідувальну інформацію, багато авторів описують цей тип OSINT як WEBINT.

Дійсно, терміни WEBINT і OSINT часто використовуються як взаємозамінні[15]. Соціальні медіа, такі як соціальні мережі, спільноти для обміну медіа та спільні проекти – це сфери, де створюється більшість користувацького контенту. Розвідка соціальних медіа або SOCMINT – це «розвіддані, зібрані з сайтів соціальних медіа». Деяка інформація з них може бути у відкритому доступі без будь-якої автентифікації, необхідної для проведення розслідування[16].

Компанія **«Reuser's Information Service» (RIS)**[17] фокусує увагу на численних маніпуляціях з цим поняттям та зазначає OSINT є комплексною, інтегрованою

[6] Hobbs Ch, Morgan M, Salisbury D (2014) Open source intelligence in the twenty-first century. Palgrave, pp. 1–6.

[7] Там само.

[8] Там само.

[9] Kapow Software (2013) http://www.kofax.com/go/kapow/wp-building-your-osint-capability.

[10] Fleisher C (2008) OSINT: its implications for business/competitive intelligence analysis and analysts. Inteligencia Y Seguridad 4:115–141

[11] Chauhan S, Panda K (2015) Open source intelligence and advanced social media search. Hacking web intelligence open source intelligence and web reconnaissance concepts and techniques. Elsevier, pp. 15–32.

[12] Burwell HP (2004) Online competitive intelligence: increase your profits using cyber-intelligence. Facts on Demand Press, Tempe, AZ

[13] Clark RM (2004) Intelligence analysis: a target-centric approach. CQ Press, Washington, DC Danowski JA (2011) Counterterrorism mining for individuals semantically-similar to watchlist members. In: Kock Wiil U (ed) Counterterrorism and open source intelligence. Springer Berlin Heidelberg, pp. 223–247. doi:10.1007/978-3-7091-0388-3_12

[14] Boncella RJ (2003) Competitive intelligence and the web. Commun AIS 12:327–340

[15] Chauhan S, Panda K (2015) Open source intelligence and advanced social media search. Hacking web intelligence open source intelligence and web reconnaissance concepts and techniques. Elsevier, pp. 15–32.

[16] Omand D, Miller C, Bartlett J (2014) Towards the discipline of social media intelligence (2014). In: Hobbs, Morgan, Salisbury (eds.) Open source intelligence in the twenty-first century. Palgrave, 24–44.

[17] Reuser, A.H.P. (2017). The RIS Open Source Intelligence Cycle. The Journal of Mediterranean and Balkan Intelligence, 10 (2), 29-43.

У правоохоронних органах це важливий елемент системи, оскільки докази визначають, чи буде особі пред'явлено звинувачення у вчинені злочину[64] і наскільки успішним буде судовий розгляд справи.

Лінделауф з колегами[65] досліджували структурні особливості таємних злочинних мереж, використовуючи характеристику компромісу між секретністю та інформаційними можливостями таємних мереж для визначення топології злочинних мереж. Вони застосували цю методику до доказів у розслідуванні вибуху на Балі, здійсненого Джемаа Ісламією, а також до мереж розповсюдження героїну в Нью-Йорку. Дановскі[66] розробив методологію, що поєднує аналіз текстів і аналіз соціальних мереж, для пошуку осіб на дискусійних форумах, які мають дуже схожі семантичні мережі на основі змісту повідомлень, що спостерігаються членами списку спостереження, або на основі інших стандартів, таких як радикальний зміст, витягнутий з повідомлень, які вони поширюють в Інтернеті. У сфері протидії кібертероризму та підбурюванню до насильства Дановскі використовував пакистанський дискусійний форум з різноманітним контентом для отримання розвідувальної інформації про протиправну поведінку. Інші дослідники та фахівці[67] представили уніфіковане рішення з інтелектуального аналізу даних для вирішення проблеми аналізу авторства в анонімних текстових повідомленнях, таких як спам і поширення шкідливого програмного забезпечення, а також для моделювання стилю письма підозрюваних в контексті кіберзлочинної поведінки.

Бретінгхем[68] запропонував комплексну обчислювальну структуру для мережевого аналізу даних про спільні злочини, яка поєднує формальне моделювання даних з аналізом великих масивів даних про злочинність і тероризм, *«спрямованим на виявлення загальних і корисних закономірностей»*. Петерсен з колегами[69] запропонували алгоритм видалення вузлів в контексті кібер-тероризму для видалення ключових вузлів терористичної мережі. Фаллах[70] запропонував стратегію на основі теорії ігор з використанням концепції рівноваги Неша для обробки складних сценаріїв DoS-атак. Чонка з іншими фахівцями[71] запропонували рішення за допомогою Cloud TraceBack (CTB) для пошуку джерела DoS-атак і представили використання мережі з нейтральним зворотним поширенням, названої Cloud Protector, яка була навчена виявляти і фільтрувати трафік таких атак. Mukhopadhyay з колегами[72] запропонували використовувати мережу байєсівських переконань з підтримкою Copula для оцінки та кількісної оцінки кібер-ризиків та кібер-вразливостей.

Таким чином, кримінологічні підходи включають надзвичайно широкий спектр обчислювальних методів для ідентифікації:

1. *Закономірностей і нових тенденцій*
2. *Генераторів злочинності та атракторів злочинності*
3. *Соціальних і просторових мереж тероризму, організованої злочинності та банд*
4. *Мережі спільних злочинів*

[64] Gottschalk P, Filstad C, Glomseth R, Solli-Sæther H (2011) Information management for investigation and prevention of white-collar crime. Int J Inf Manage 31:226–233.

[65] Lindelauf R, Borm P, Hamers H (2011) Understanding terrorist network topologies and their resilience against disruption. In: Kock Wiil U (ed.) Counterterrorism and open source intelligence. Springer, Vienna, pp 61–72. doi:10.1007/978-3-7091-0388-3_5.

[66] Danowski JA (2011) Counterterrorism mining for individuals semantically-similar to watchlist members. Kock Wiil U (ed) Counterterrorism and open source intelligence. Springer Berlin Heidelberg, pp. 223–247. doi:10.1007/978-3-7091-0388-3_12.

[67] Iqbal F, Binsalleeh H, Fung BCM, Debbabi M (2013) A unified data mining solution for authorship analysis in anonymous textual communications. Inf Sci 231:98–112.

[68] Brantingham PL (2011) Computational Criminology. 2011 European intelligence and security informatic conference. IEEE Computer Society. doi:10.1109/EISIC.2011.79.

[69] Petersen RR, Rhodes CJ, Kock Wiil U (2011) Node removal in criminal networks. 2011 European intelligence and security informatics conference. IEEE Computer Society, pp. 360–365.

[70] Fallah M (2010). A puzzle-based defence strategy against flooding attacks using game theory. IEEE Trans Dependable Secure Comput 7:5–19.

[71] Chonka A, Xiang Y, Zhou W, Bonti A (2011) Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. J Netw Comput Appl 34:1097–1107.

[72] Mukhopadhyay A, Chatterjee S, Saha D, Mahanti A, Sadhukhan SK (2013) Cyber-risk decision models: To insure IT or not? Decis Support Syst 56:11–26. http://dx.doi.org/ 10.1016/j.dss.2013.04.004.

Потрібно зазначити, що сучасні моделі та методи постіно розвиваються та удосконалюються.

Хоча багато підходів здаються корисними для розслідування кіберзлочинів, існуюча література свідчить про те, що аналіз соціальних мереж, інтелектуальний аналіз даних, аналіз текстів, кореляційні дослідження та методи оптимізації, особливо з акцентом на аналізі великих обсягів даних з відкритих джерел, є найбільш практичними методами.

ВИСНОВКИ

Зростання кіберзлочинності становить велику небезпеку для громадської безпеки та добробуту, створюючи постійні виклики для правоохоронних органів, оскільки інструменти, що використовуються окремими особами та групами осіб для вчинення злочинів, та вектори, за допомогою яких вони вчиняють злочини, продовжують розвиватися. Право на анонімність, широкий спектр додатків/пристроїв для доступу до інтернету, а також інші проблеми, пов'язані з міжнародною юрисдикцією, технологічними змінами, навчанням, освітою та обізнаністю, продовжують посилювати серйозність викликів, з якими стикаються ті, на кого покладено обов'язок захищати суспільство та його громадян. Постійне поширення підключених пристроїв, від традиційних комп'ютерів до мобільних пристроїв та інтернету речей, означає, що молоді та вразливі особи мають доступ до інтернету, як ніколи раніше, створюючи нові вектори для експлуатації та зловживань.

Вплив кіберзлочинності змусив розвідувальні та правоохоронні органи всього світу боротися з кіберзагрозами. Перед усіма секторами зараз стоять схожі дилеми: як найкраще пом'якшити наслідки кіберзлочинності і як ефективно сприяти безпеці людей і організацій. Отримання унікальних і цінних розвідувальних даних шляхом збору публічних записів для створення всебічного профілю певних цілей швидко стає важливим засобом для розвідувального співтовариства. Оскільки кількість доступних відкритих джерел швидко зростає, протидія кіберзлочинності все більше залежить від передових програмних засобів і методів збору та обробки інформації в ефективний і результативний спосіб.

РОЗДІЛ 4

ГЛОБАЛЬНА ТРАНСФОРМАЦІЯ OSINT: МІЖНАРОДНІ КЕЙСИ, ЩО ЗМІНИЛИ ПРАВИЛА ГРИ

Михайло ВЕРИЧ

Незалежно від того, чи готові до цього окремі особи та організації, чи ні, нові можливості та виклики, пов'язані з відкритою інформацією з різних джерел, - це те, з чим нам доведеться зіткнутися зараз і в майбутньому. Слід розуміти, що цей величезний обсяг інформації з відкритих джерел в Інтернеті дозволяє будь-кому, добре це чи погано, стати розслідувачем. Те, що обирають для розслідування, може варіюватися від воєнних злочинів у далекій країні до спецпідрозділів на порозі власного будинку, і обізнаність про таку поведінку має вирішальне значення в багатьох аспектах. Також розробляється багато нових інструментів для приватних осіб та організацій у державному та приватному секторах, які мають на меті полегшити процес розслідування з використанням відкритих джерел, чи то для того, щоб знайти інформацію, чи то для того, щоб організувати її у більш доступну форму.

За останні кілька років сфера розслідувань з використанням відкритих джерел

пережила своєрідний ренесанс. Цьому сприяли події Арабської весни, коли соціальні мережі спочатку використовувалися під час протестів, а згодом – медіа-активістами та озброєними групами, які брали участь у конфліктах, що виникли внаслідок цих протестів. У цей період окремі особи та організації почали вивчати способи дослідження величезного обсягу інформації, що надходила з цих країн, і для вивчення цієї інформації використовували нові інструменти та платформи.

Після Арабської весни ті ж самі навички і методи, набуті в цей період, почали застосовуватися до нових конфліктів і ситуацій. Підозри щодо причетності росії до інцидентів в Україні опинилися під пильною увагою після збиття літака рейсу 17 Малайзійських авіаліній (MH17) 17 липня 2014 року, а інформація з відкритих джерел, зокрема з соціальних мереж, стала ключовим джерелом інформації в публічних дебатах про те, що сталося з MH17. Водночас, пости в соціальних мережах від місцевих жителів на сході України та в прикордонних з Україною регіонах росії були використані для викриття військової агресії росії на територію України.

За останні кілька років особливо помітним стало те, що доступ до нового спектру онлайн-інструментів зробив розслідування з відкритими джерелами тим, що будь-хто може робити, не виходячи з дому. Завдяки Google та іншим компаніям, що надають технічні послуги, тепер можна отримати доступ до супутникових знімків всієї планети, фотографій з географічною прив'язкою з усього світу, вуличних знімків з тисяч локацій у десятках країн, а також до величезного обсягу відеоконтенту з усіх куточків Землі.

Лише за допомогою цих інструментів будь-хто може стати дослідником відкритих джерел, а нові (і часто безкоштовні) інструменти та платформи створюються і швидко приймаються зростаючою публічною онлайн-спільнотою дослідників відкритих джерел. Незалежно від того, чи адаптуються професіонали, які працюють у цій сфері, до цих нових змін чи ні, очевидно, що громадський рух, який зростає, вже використовує цю інформацію.

Інформацію з відкритих джерел вже використовують у своїй роботі різноманітні новинні та правозахисні організації. Наприклад, у 2013 році газета New York Times використала відеоматеріали, розміщені в Інтернеті сирійськими збройними опозиційними групами, щоб ідентифікувати зброю, яку іноземні уряди контрабандним шляхом постачали сирійській опозиції, викриваючи те, що мало бути вкрай секретною операцією, завдяки відео на YouTube[1]. **Human Rights Watch і Amnesty International** тепер використовують відеоматеріали, зібрані з соціальних мереж, у поєднанні з супутниковими знімками і особистими інтерв'ю для встановлення фактів, пов'язаних з широким спектром подій. Наприклад, у червні 2014 року Human Rights Watch використовувала супутникові знімки в поєднанні з відео, розміщеними в Інтернеті Ісламською державою, щоб знайти точне місце масових страт у Тікріті, Ірак[2].

Нещодавно спроби організувати величезну кількість інформації, що надходить з відкритих джерел у зонах конфліктів, призвели до створення таких платформ, як PATTRN від кафедри судової архітектури Університету Голдсміта[3], яка використовується для розміщення платформи Amnesty International по Газі[4], і таких проектів, як Сирійський архів[5]. Ці проекти збирають величезну кількість інформації з відкритих джерел, що надходить з різних нових джерел, і намагаються організувати її так, щоб зробити інформацію більш доступною. Це дозволяє користувачам отримати глибше розуміння конфлікту без необхідності проводити тривалі дослідження, необхідні для впорядкування хаосу цих нових джерел відкритої інформації.

[1] http://www.nytimes.com/2013/02/26/world/middleeast/in-shift-saudis-are-said-to-arm-rebels-in-syria.html
[2] https://www.hrw.org/news/2014/06/26/iraq-isis-execution-site-located.
[3] http://www.gold.ac.uk/news/pattrn/.
[4] http://gazaplatform.amnesty.org/.
[5] https://syrianarchive.org/.

мережах. Наприклад, у листопаді 2015 року під час антитерористичної операції в Брюсселі місцевих жителів попросили не поширювати фотографії з місця подій. Багато знімків, зроблених громадянами, поширювалися в соціальних мережах з хештегом *#BrusselsLockdown*, і у відповідь на прохання не ділитися зображеннями користувачі соціальних мереж почали наповнювати хештег фотографіями котів. Це призвело до того, що попередні фотографії поліцейських операцій, якими ділилися за цим хештегом, були заглушені величезною кількістю фотографій котів, а також до позитивного висвітлення події у ЗМІ[15]. У відповідь на імпровізовану кампанію громадськості в соціальних мережах федеральна поліція Бельгії відповіла подякою у Твіттері - мискою котячого корму з підписом *«Для всіх тих котів, які допомогли нам вчора... будь ласка!»*[16].

Хоча не всі розслідування та дослідження з використанням відкритих джерел підходять для краудсорсингу або залучення громадськості, це свідчить не лише про можливість застосування цієї технології, але й про те, що зростає спільнота людей, зацікавлених у розслідуванні з використанням відкритих джерел, які готові присвятити свій вільний час участі в краудсорсингових проектах, а також про те, що з'являється все більше безкоштовних і недорогих інструментів, які дають таким людям можливість це робити.

Інструментарій розслідувань з використанням відкритих джерел постійно розширюється, спираючись на інформацію зі все більшої кількості соціальних мереж і платформ для обміну даними, які, в свою чергу, постійно наповнюються все більшим обсягом контенту з глобального ринку смартфонів, що розширюється. Обмін фотографіями швидко поширився на обмін відео, а додатки для перегляду відео в прямому ефірі стають дедалі популярнішими. Такі платформи, як Yomapic, WarWire, EchoSec та інші, тепер пропонують недорогі варіанти пошуку географічно прив'язаних зображень і відео, розміщених на сайтах соціальних мереж, що дозволяє будь-кому знаходити зображення з місця подій майже в реальному часі, що все частіше використовується при висвітленні екстрених новин.

Змінюється не лише ситуація на поверхні землі, а й ситуація у космосі. Щороку запускається все більше супутників, що збільшує кількість безкоштовних супутникових знімків на різних платформах, знижуючи ціни на комерційні супутникові знімки. Відео з високою роздільною здатністю з супутників також буде ставати все більш поширеним, а використання супутникових знімків слідчими стає все більш поширеним.

Завдяки новим інструментам і ресурсам розслідування з відкритих джерел стали безцінним джерелом інформації для тих, хто розслідує величезне коло тем і з величезного кола причин. Останніми роками правозахисні організації, активісти та журналісти взяли на озброєння ці нові інструменти та ресурси, і вже зараз зрозуміло, що розслідування за допомогою відкритих джерел стане ключовою частиною роботи багатьох розслідувачів, незалежно від їхнього досвіду.

ВИСНОВОК

Незалежно від того, чи готові до цього окремі особи та організації, чи ні, нові можливості та виклики, пов'язані з відкритим доступом до інформації з різних джерел - це те, з чим нам доведеться зіткнутися зараз і в майбутньому. Стрімке поширення технології смартфонів призвело до того, що фотоапарат опинився в кишені кожного, дозволяючи людям миттєво ділитися майже кожною миттю свого існування. Завдяки підключенню до Інтернету ми всі можемо отримати доступ до цієї інформації з будь-якої точки світу, тому виклик, з яким ми стикаємося, полягає в тому, щоб зрозуміти, як це впливає на нашу роботу і як ми можемо використовувати цю інформацію у власній роботі. Слід розуміти, що

[15] https://www.buzzfeed.com/stephaniemcneal/brussels-lockdown-cat-pictures?utm_term=.nk7qY 56nK#.qybXjr0Ld.
[16] https://twitter.com/FedPol_pers/status/668749104655302656.

цей величезний обсяг інформації з відкритих джерел в Інтернеті дозволяє будь-кому, добре це чи погано, стати розслідувачем.

Також розробляється багато нових інструментів для приватних осіб та організацій у державному та приватному секторах, які мають на меті полегшити процес дослідження відкритих джерел, чи то для пошуку інформації, чи то для організації знайденої інформації у більш доступний спосіб.

"Інформація – це боєприпас. Але лише аналітика робить її зброєю" -

Авторська формула

У сучасному світі, де дані множаться з неймовірною швидкістю, саме аналітика – структурована, етична, інституціоналізована – перетворює інформаційний шум на точкову дію. OSINT, як відкритий інструмент збору, не має сили без процесу перевірки, інтерпретації та впровадження. Ця частина монографії присвячена тому, як держава, інституції та фахівці можуть перетворити інформаційний потенціал на оперативну перевагу – через методологію, інфраструктуру та перспективу інтеграції.

ІНСТИТУЦІОНАЛІЗАЦІЯ OSINT В ОПЕРАТИВНОМУ УПРАВЛІННІ: методологія, інфраструктура, перспективи

ЧАСТИНА ІІ

РОЗДІЛ 5
ПРОЦЕС ЯК МЕТОДОЛОГІЯ OSINT

Олександр КОРИСТІН

Там, де різним організаціям необхідно об'єднати зусилля в критично важливих ситуаціях для досягнення низки спільних цілей, завдань і результатів, без єдиного і спільного розуміння і підходу до того, як обробляти, аналізувати, розуміти і діяти на основі інформації, як це передбачено належним інформаційним врядуванням, ймовірність невдачі або менш ефективних результатів у досягненні цих цілей, завдань або результатів є надзвичайно високою. Це пов'язано з ризиком того, що різні залучені організації та відомства можуть приймати суперечливі або неефективні рішення внаслідок різного тлумачення розвідувальних даних або різного реагування на них, що зумовлено їхніми різними організаційними підходами і поглядами на світ, в якому вони існують і діють.

Простіше кажучи, прийняття стратегічних і тактичних рішень у військовій чи цивільній сферах, або у спільному просторі, що відбувається під час значних кризових ситуацій, надзвичайних ситуацій або серйозних подій чи операцій, пов'язаних з організованою злочинністю чи тероризмом, вимагає збору даних з усіх наявних відповідних джерел - технічних і людських - як з відкритих (наприклад, соціальні мережі, Інтернет і комерційні ресурси), так і з закритих (військові або інші специфічні) джерел. Потім необхідна критична обробка, під час якої відбувається аналіз, щоб перетворити розрізнену, неоднозначну інформацію з різних джерел на придатну для використання, змістовну, достовірну, точну і своєчасну розвідувальну інформацію. Потім для подальшого розповсюдження серед відповідних кінцевих користувачів. Механізм зворотного зв'язку потрібен для перевірки і підтвердження точності, а також, за необхідності, для визначення «найкращої» метрики. Все це повинно вписуватися в єдину і загальну систему управління інформацією, щоб гарантувати, що незалежно від різного бачення світу кожною організацією, всі розглядають отримані дані і потреби в прийнятті рішень з єдиної і спільної точки зору. Це може призвести до прийняття більш обґрунтованих рішень.

У складному середовищі міжвідомчої взаємодії, де рішення приймаються під тиском часу, ризиків і неоднозначності, критично важливою стає узгодженість у підходах до збору, обробки та аналізу інформації. Відсутність єдиної методології може призвести до фрагментації дій, суперечливих інтерпретацій і втрати ефективності. Саме тому OSINT, як інструмент аналітичної розвідки, потребує чіткості процесу – з урахуванням потреб замовника, етичних стандартів, технологічних викликів і гнучкості в адаптації до різних контекстів. Від класичних розвідувальних циклів до бізнес-моделей і модульних підходів – кожна методологія пропонує унікальну логіку, яка може бути інтегрована в національну практику.

Саме тут важливо описати цикл або процес розвідки, як він підтримує прийняття рішень, а також проблеми і виклики, з якими стикається OSINT як невід'ємна частина цього комплексу і циклу. На думку фахівців[1] розвідувальний цикл складається з шести фаз: (1) спрямування; (2) збір; (3) обробка; (4) аналіз; (5) поширення і (6) зворотний зв'язок (*рис. 1*).

1. **Спрямування.** Вимоги і потреби в розвідці визначаються особою, яка приймає рішення, для досягнення цілей. В НАТО командувач використовує вимоги (іноді їх називають *«Основні елементи розвідки»* (EEI) 'Essential Elements of Intelligence (EEIs)) для того, щоб розпочати розвідувальний цикл.

[1] Akhgar, B., Bayerl, P., Sampson, F. (eds) Open Source Intelligence Investigation. Advanced Sciences and Technologies for Security Applications. Springer, Cham., 2016. https://doi.org/10.1007/978-3-319-47671-1_6

Рисунок 1. Процес/цикл розвідки

2. **Збір.** У відповідь на вимоги співробітники розвідки розробляють план збору розвідувальної інформації, використовуючи наявні джерела і методи, а також запитуючи розвідувальну інформацію в інших відомствах. Збір розвідувальної інформації включає дані з кількох напрямів збору розвідувальної інформації, таких як HUMINT, IMINT, ELINT, SIGINT, а також OSINT. Це називається *«колекція»*.

3. **Обробка.** Після того, як план збору виконаний і інформація отримана, її обробляють для використання. Це передбачає переклад необроблених розвідувальних матеріалів, досить часто з іноземної мови, оцінку релевантності та достовірності, а також зіставлення необроблених розвідувальних даних для підготовки до використання.

4. **Аналіз.** Аналіз встановлює значення і наслідки оброблених розвідувальних даних, інтегрує їх, поєднуючи розрізнені частини інформації для виявлення супутньої інформації і закономірностей, а потім інтерпретує значення будь-якого нового знання, що з'явилося.

5. **Поширення.** Готові розвідувальні продукти приймають різні форми залежно від потреб особи, яка приймає рішення, і вимог до звітності. Рівень терміновості різних видів розвідданих зазвичай встановлюється розвідувальною організацією або спільнотою. Наприклад, бюлетень з вказівками і попередженнями вимагає більш високого пріоритету, ніж річний звіт. Це називається поширенням.

6. **Зворотний зв'язок.** Цикл розвідки не є замкнутим. Від особи, яка приймає рішення, та інших джерел надходить зворотній зв'язок, і видаються переглянуті вимоги.

Отже, в контексті вищесказаного, якщо уявити сучасний стан збору, обробки, аналізу і поширення цих даних - розвідувальний цикл - у вигляді воронки, що дедалі звужується, з експоненціальним зростанням джерел і попиту на OSINT як невід'ємну частину цього процесу, то критична обробка і аналіз, де інформація перетворюється на придатні для використання розвідувальні дані, стали значно вужчим місцем.

У подальшому аналізі важливим є порівняння зазначеного процесу (циклу) OSINT з методологією, розробленою для бізнесу, тобто проведення OSINT розслідувань

в інтересах бізнесу, яка отримала назву **CRAWL**: *Communicate, Research, Analyze, Write, and Listen* (спілкуйся, досліджуй, аналізуй, пиши і слухай)[2].

І хоча ці дві методології схожі, вони мають дві основні відмінності:

По-перше, CRAWL зосереджується на бізнес-розслідуваннях, які проводять приватні професійні детективи, на відміну від розвідки, яку проводять представники державних органів, яку зазвичай називають розвідкою.

По-друге, CRAWL в основному стосується дослідницької спільноти в Інтернеті, яка з часом розвинула вузькоспеціалізовану експертизу, яку зазвичай називають *«OSINT»* - розвідка з відкритих джерел. Цей термін був запозичений розвідувальним співтовариством з часів до Інтернету, коли він зазвичай означав розвіддані, зібрані з офлайнових медіа-джерел, таких як радіопередачі і газети.

Як зазначають автори, різниця між цими двома методологіями ледь помітна, але водночас і велика. CRAWL визначає вдосконалений підхід до OSINT як спосіб пошуку та аналізу даних, який додає важливі елементи до розмови - це бізнес-модель для розслідувачів, так само як *«науковий метод»* - для науковців[3].

Важливо звернути увагу на CRAWL і зрозуміти, що ця методологія, на думку авторів, чітко показує, що це не є магією, так як вона не приховується і прозорими є підходи до роботи. На противагу, коли *«приховується»* професія, відкриваються двері для людей, які можуть запідозрити у незаконній діяльності. CRAWL - це спосіб утвердити ремесло як щось етичне, серйозне і успішне.

CRAWL починається з - *комунікації («C» - Communicate)*. Все починається з чіткої комунікації. Повідомляється про те, що буде зроблено, а що не може бути зроблено, створюючи належний лист-зобов'язання, із врахуванням юридичних зобов'язань та етики професії.

Наступний етап - *дослідження (R: Research)*. Це процес, який постійно змінюється і вимагає творчого підходу. Дослідження включає в себе те, що робиться в інтернеті, особисто, а також всі інші важливі вимоги до збору даних, які допоможуть відповісти на питання *«чому»*. Зважаючи на потік доступної інформації, це не тільки важливо, але й складно. Зараз, в епоху ШІ (штучного інтелекту), збір даних здається простішим, ніж будь-коли, але водночас і більш підозрілим.

Але дослідження вимагає наступного етапу *«аналізу»* - необхідно перетворити знайдені дані на знання. Аналіз (A: Analyze) - це не просто підсумовування даних. Це поєднання наукової та ненаукової інтерпретації даних для отримання розумних, глибоких висновків. Дослідження приносить дані, а аналіз перетворює ці дані на знання.

Наступним кроком у CRAWL є *«написання»* - *писати (W: Write)*. Створення письмового звіту для клієнта має відбуватися відповідно до очікувань, які були встановлені під час призначення проекту. Основними складовими кожного звіту є повторне формулювання мети, результати дослідження та рекомендації. Також додається інформація про метод пошуку та важлива контактна інформація. Звіти повинні бути неупередженими і без надмірного охоплення.

Певним чином унікальний етап цієї методології є - *слухати (L: Listen)*. Так як це бізнес-модель, для неї важливим є спілкування з клієнтом-замовником, як щодо мети і завдань, так і щодо повноти виконаної роботи та належності аналізу. Це також про вивчення досвіду інших експертів у цій галузі, дослідження літератури, відвідування курсів тощо. Це завершальний етап процесу.

Порівнюючи різноманітні підходи до методології OSINT, неможливо оминути напрацювання компанії *«Reuser's Information Service»* (RIS), де наголошується, що стандартний цикл розвідки (intelligence cycle) не відповідає потребам OSINT-дослідження, оскільки кількість кроків такого дослідження може змінюватись

[2] Hetherington C., OSINT: The Authoritative Guide to Due Diligence. Hetherington Group, 2024
[3] Там само

організації роботи, перегляду робочих процесів.

ВИСНОВОК

Різноманіття підходів до OSINT не є слабкістю, а навпаки – джерелом сили, що дозволяє адаптувати інструменти до конкретних завдань, контекстів і етичних вимог. Визначальними стають не лише технічні засоби, а й здатність мислити системно, комунікувати прозоро, зберігати знання та будувати довіру між аналітиком і замовником. Інституалізація OSINT як методології – це не просто впровадження інструментів, а формування культури аналітичної розвідки, де зміст переважає над формою, а синтез знань – над механічним аналізом.

Попри відмінності у структурі – від формалізованої лінійності класичного циклу, через етичну комунікаційну модель **CRAWL**, до модульної гнучкості **RIS** – усі методології демонструють єдність у принципових складових:

- **циклічність:** *OSINT – це не одноразова дія, а повторюваний процес уточнення, перевірки та вдосконалення;*
- **орієнтація на замовника:** *потреби замовника визначають напрям дослідження, структуру процесу та формат результату;*
- **комунікація як основа:** *чітке формулювання завдання – ключ до релевантного і корисного аналітичного продукту;*
- **обробка та аналіз як вузьке місце:** *саме тут перетворюється інформація на знання, і саме тут виникає найбільше викликів;*
- **етичність і прозорість:** *відповідальність за процес, джерела та результати – фундамент довіри до OSINT.*

Спільним знаменником є також те, що OSINT не функціонує як автономна або самодостатня діяльність. Його цінність визначається здатністю генерувати релевантну, достовірну та своєчасну інформацію, яка інтегрується в управлінський контекст і слугує основою для прийняття стратегічних або тактичних рішень. Таким чином, OSINT слід розглядати не як інструмент збору даних, а як елемент аналітичної інфраструктури, що забезпечує обґрунтованість, адаптивність і легітимність управлінських дій у складному інформаційному середовищі.

РОЗДІЛ 6

ІНФРАСТРУКТУРА ЗБОРУ OSINT-ДАНИХ: ДЖЕРЕЛА, ФОРМАТИ ТА МЕТОДИ ПІДГОТОВКИ

Юрій КАРДАШЕВСЬКИЙ

Ефективне використання відкритих джерел інформації в оперативно-розшуковій та аналітичній діяльності потребує чітко структурованої інфраструктури збору даних, яка враховує різноманіття форматів, джерел та методів доступу. У контексті цифрової трансформації суспільства, де значна частина людської активності переміщується в онлайн-простір, відкриті дані набувають стратегічного значення для правоохоронних органів. Проблематика полягає не лише в обсязі доступної інформації, а й у складності її вилучення, перевірки, структурування та інтеграції в аналітичні процеси. Відсутність уніфікованих процедур, обмеження доступу до API, епізодичність даних із соціальних мереж, а також ризики дезінформації створюють додаткові виклики для слідчих та

аналітиків. Тому критично важливо розглядати OSINT не як технічну функцію збору, а як елемент управлінської екосистеми, що забезпечує обґрунтованість і адаптивність рішень у складному інформаційному середовищі.

В основі всіх розвідувальних розслідувань з відкритих джерел лежать дані. НАТО поділяє інформацію та розвіддані з відкритих джерел на чотири категорії[1]: *дані з відкритих джерел; інформація з відкритих джерел; розвіддані з відкритих джерел (OSINT); перевірені розвіддані з відкритих джерел*. НАТО визначає кожну з цих категорій по-різному, водночас, розвідка з відкритих джерел є найбільш придатною для розслідувань правоохоронних органів.

За оцінками **Pallaris**[2], від 80 до 95% всієї інформації, що використовується розвідувальною спільнотою, надходить з відкритих джерел. Для правоохоронних органів це може бути перебільшеним твердженням, однак, зважаючи на те, що значна частина людського життя проходить в Інтернеті, OSINT стає все більш важливим ресурсом у боротьбі зі злочинністю.

Здається, існує два чіткі кінці спектру щодо збору даних з відкритих джерел. З одного боку, це надзвичайно специфічний ручний пошук джерел, таких як Інтернет і соціальні мережі, можливо, з метою відстеження конкретної особи або конкретної інформації про неї, як це робили учасники **Bellingcat**[3]. На іншому кінці спектра - набагато масштабніші, хоча й цільові, розслідування, в яких слідчі можуть бути зацікавлені в обговоренні певної теми або події, що має безпосереднє відношення до їхнього розслідування, але не обов'язково володіють конкретною інформацією, яку вони шукають.

Причини, з яких слідчий може захотіти отримати інформацію з відкритих джерел, є широкими та різноманітними. Це може бути пов'язано з тим, що така інформація недоступна через звичайні канали закритої розвідки, вона може бути необхідна для того, щоб визначити напрямок пошуку закритої розвідки, або ж слідчий не хоче відмовлятися від джерела своєї закритої розвідки і тому вдається до відкритих джерел для пошуку тієї ж інформації[4]. У багатьох організаціях отримання розвідувальної інформації регулюється циклом розвідки, що реалізується на основі відповідної методології.

Важливо розуміти, що ретельне планування визначення даних, що стосуються питань розслідування, на які потрібно відповісти, і процесів отримання таких даних є важливим і водночас вирішальним першим кроком для отримання розвідувальної інформації необхідної якості і точності. Фахівці оцінюють, що від 50 до 80 % їхнього часу може бути витрачено саме на ці процеси та складові збору даних: тобто на зусилля зі збору потрібних даних[5], перетворення їх у необхідний для аналізу формат, поєднання з іншими джерелами даних (як відкритими, так і закритими), визначення релевантних даних, а також на початок процесів вилучення та агрегування даних.

У досудовому розслідуванні слідчі вживають необхідних заходів для виявлення та закріплення доказів, які мають відношення до провадження. Це може бути інформація від свідків, потерпілих і підозрюваних, а також судово-медична інформація з місця події, попередні розвідувальні дані про осіб і відповідні локації, а також доступ до даних з пасивних генераторів даних, таких як камери відеоспостереження і банківські записи тощо. Більш ніж будь-коли дані з відкритих джерел можуть доповнити цю інформацію і надати життєво важливі докази, які можуть допомогти у вирішенні справи, якщо їх правильно ідентифікувати, вилучити, опрацювати, проаналізувати і представити.

[1] NATO (2001) NATO open source intelligence handbook

[2] Pallaris C (2008) Open source intelligence: a strategic enabler of national security. CSS Analyses Secur Policy 3(32):1–3

[3] https://www.bellingcat.com/

[4] Gibson S (2004) Open source intelligence. RUSI J 149:16–22

[5] Lohr S (2014) For big-data scientists, "Janitor Work" is key hurdle to insights. In: The New York Times. http://mobile.nytimes.com/2014/08/18/technology/for-big-data-scientists-hurdle-to-insights-is-janitor-work.html?_r=2

По-друге, особиста інформацію в Інтернеті, як правило, достатньо тонко редагується, забезпечуючи особистий захист та конфіденційність[66]. По-третє, навмисне зловмисне поширення дезінформації є набагато серйознішою справою і може розглядатися як спроба навмисного перешкоджання виявленню в Інтернеті або спрямування слідства в хибному напрямку, щоб відвернути інтерес або завадити слідству встановити зв'язок між спільниками.

Програмні засоби для збору та підготовки даних

Багато дослідників з відкритих джерел не можуть покладатися на певні інструменти, або не в змозі створити їх самостійно. Існує низка як комерційних, так і загальнодоступних інструментів, які можуть допомогти в цьому процесі. Використовуючи готові інструменти, розслідувачі можуть втратити деякий тонкий контроль над інформацією, до якої вони отримують доступ і яку здобувають, однак це може компенсуватись швидкістю виконання цього процесу.

Комерційні інструменти, які можуть здійснювати збір і підготовку даних з відкритих джерел, включають **i2 Analyst Notebook**[67], **Maltego** і **CaseFile**[68], **Palantir**[69] і **AxisPro**[70]. Хоча Maltego описується як такий, що не забезпечує більшого результату *«ніж це може зробити людина з технічними навичками і браузером»*, той же автор також зазначає, що *«його краса полягає в здатності до масштабування»*[71]. Кожен з цих інструментів містить методи для збору даних як в режимі реального часу, так і для імпорту офлайн-даних, а також для вилучення сутностей і моделювання зв'язків, поглибленого аналізу та візуалізації. Отже, ці інструменти призначені не лише для збору даних та вилучення інформації, але вони дійсно впливають на кожен крок у розвідувальному циклі.

Окрім комерційних інструментів, зараз все більше з'являється програмного забезпечення з відкритим кодом, яке можна використовувати з невеликими витратами або взагалі без них (як у фінансовому, так і в ресурсному плані). Водночас, набір інтернет-інструментів з відкритим вихідним кодом також надає функцію вилучення даних під час перегляду веб-сторінок, що дозволяє легко завантажувати контент[72]. Плагін **DataWake** для **Firefox**[73], який є частиною каталогу Memex, спостерігає за тим, як ви переглядаєте веб-сторінки, фіксуючи сайти, на які ви переходите, а також деякі організації, присутні на їхніх сторінках.

На завершення, незважаючи на те, що розслідувачі, природно, хочуть отримати потрібну їм інформацію якомога швидше, як відповідальний користувач Інтернету, навіть розслідувачі повинні отримувати дані тільки таким чином, щоб поважати інших; особливо тому, що творець веб-контенту не обов'язково збігається з особою (особами), які керують сайтом і платять за пропускну здатність, доступ до сервера тощо.

ВИСНОВОК

Інфраструктура збору OSINT-даних є багатовимірною системою, що поєднує технологічні інструменти, методологічні підходи та етичні стандарти. Її ефективність визначається не лише здатністю ідентифікувати релевантні джерела, а й спроможністю трансформувати неструктуровану інформацію у придатні для аналізу формати, інтегрувати її з іншими типами даних та забезпечити її валідацію. Усе це має слугувати не накопиченню інформації, а підтримці процесу прийняття рішень: стратегічного, оперативного чи

[66] Bayerl PS, Akhgar B (2015) Surveillance and falsification implications for open source intelligence investigations. Commun ACM 58(8):62–69
[67] http://www-03.ibm.com/software/products/en/i2-analyze
[68] https://www.paterva.com/web6/
[69] https://www.palantir.com/
[70] http://www.textronsystems.com/products/advanced-information/axis-pro
[71] Bradbury D (2011) In plain view: open source intelligence. Comput Fraud Secur 2011(4):5–9
[72] http://osirtbrowser.com/
[73] http://sotera.github.io/Datawake/

тактичного. Саме тому OSINT слід розглядати як інтелектуальну інфраструктуру, що формує основу для проактивного реагування, прогнозування ризиків та побудови довіри в системі безпеки

РОЗДІЛ 7

МОДЕЛІ АНАЛІЗУ ТА ПЕРЕВІРКИ OSINT: ВІД БАГАТОКАНАЛЬНОЇ АНАЛІТИКИ ДО ДОСТОВІРНОЇ ІНТЕРПРЕТАЦІЇ

Олександр КОРИСТІН

У сучасному середовищі відкритих джерел інформації ефективне перетворення даних на розвідувальні продукти вимагає не лише збору, а й глибокої аналітичної обробки, перевірки та контекстуалізації. Тому важливим є систематизований підхід до аналізу OSINT, охоплюючи текстову аналітику, мережевий аналіз, геопросторову обробку та методи верифікації. Особлива уваги заслуговують інструменти, які дозволяють досліднику не просто виявляти ключові сутності, а й будувати зв'язки, визначати достовірність і формувати цілісну картину подій. У результаті – OSINT, що є не лише багатоканальним, а й надійним, релевантним і придатним для практичного застосування.

Ключовий компонент перетворення даних та інформації з відкритих джерел на розвідувальні дані з відкритих джерел відбувається на етапах аналізу та інтерпретації. Крім того, етапи верифікації та валідації можуть перетворити OSINT на перевірену OSINT, яка має вищий ступінь достовірності. Через широкий спектр типів даних, які можна отримати з відкритих джерел інформації, методи аналізу даних, які можна застосувати до цих даних, залежить той максимум, що може отримати дослідник від цих даних, а також підготувати їх для подальшого аналізу за допомогою візуалізації та методів візуальної аналітики для вивчення та презентації.

Насправді, було сказано, що *«основна різниця між базовими та іншими "операціями" OSINT полягає в аналітичному процесі»*[1]. Крім того, етапи верифікації та валідації можуть перетворити такий OSINT на валідований OSINT, який має вищий ступінь довіри.

> *Валідований OSINT* – це інформація з відкритих джерел, яка пройшла процес верифікації та підтвердження, і має високий ступінь достовірності. Такий OSINT може бути використаний як основа для прийняття рішень або навіть як доказовий матеріал у розслідуваннях.

Через широкий спектр типів даних, які можна отримати з відкритих інформаційних джерел, залежать методи аналізу даних, які можна виконати на цих даних. Варто звернути увагу на набір загальних процесів аналізу, які можна використовувати при роботі з конкретними типами даних, незалежно від того, про що ці дані стосуються. Ці методи допоможуть досліднику відкритих джерел отримати максимум від своїх даних, а також підготувати їх для подальшого аналізу з використанням методів візуалізації та візуальної аналітики для вивчення та презентації.

МЕТОДИ АНАЛІЗУ ДАНИХ

Незважаючи на важливість текстових джерел, вони не є всією сутністю OSINT.

[1] Hribar G, Podbregar I, Ivanuša T (2014) OSINT: a "Grey Zone"? Int J Intell CounterIntell 27 (3):529–549

Часто існує значна кількість інших даних, таких як час, дата, місцезнаходження та інші метадані, які можна проаналізувати, не кажучи вже про велику кількість даних, що містяться в джерелах зображень, відео та аудіо, які набагато складніше проаналізувати. Можливо, більша складність аналізу таких даних може також принести більшу вигоду через меншу кількість організацій, здатних здобувати розвідувальну інформацію з такої інформації.

Текстовий аналіз

Значна частина відкритих джерел містить велику кількість неструктурованих текстових даних, які можна обробляти і аналізувати різними способами з метою вилучення релевантної інформації. Сучасний підхід до обробки природної мови (natural language processing - NLP) визначається фахівцями ключовим компонентом OSINT[2].

Найпростішою моделлю *обробки тексту* є модель *«мішка слів»*, коли кожне слово в кожному реченні документа (тут документ може бути будь-яким - від повнотекстового документа, статті в газеті або короткого твіту) розбивається на список слів. Потім до цього списку можна застосувати різні аналізи, починаючи з дуже простого підрахунку кількості входжень кожного окремого терміна, щоб визначити, які слова з'являються найчастіше. Це може бути використано для швидкого огляду документа за допомогою дуже простого підрахунку. Він також може слугувати основою для вилучення ключових слів.

Цю модель також можна використовувати для складніших обчислень, таких як конкорданс, що дозволяє визначити контекст, у якому певне слово вживається в документі.

> *Конкорданс* – це метод текстового аналізу, який дозволяє визначити контекст вживання певного слова або терміна в документі. Часто використовується для виявлення синонімів, тематичних зв'язків або підтвердження значення термінів у кримінологічних текстах.

Потім конкорданс можна розширити, щоб визначити інші слова, які можуть бути використані в тому ж або подібному контексті, і таким чином допомогти скласти список синонімів або збільшити кількість підтверджень, уможливлюючи виявлення різних слів, які могли бути використані для опису однієї і тієї ж події. Конкорданс також іноді називають *«ключовим словом у контексті»*[3]. Зокрема, конкорданс використовується в контексті аналізу документів, пов'язаних зі злочинністю, підкріплених візуалізаціями[4].

Ще однією перевагою використання моделі *«мішка слів»* є можливість обчислення словосполучень. Колокації визначають слова, які часто з'являються разом, визнаючи, що іноді це більш корисно, ніж окремі слова.

Більш досконалою моделлю, ніж модель мішка слів, є *модель векторного простору*. Ця модель аналізує документи як частину масиву, тобто як частину набору документів, визначаючи всі окремі терміни в масиві і для кожного документа в масиві надаючи кожному слову рейтинг. Найпоширенішою формою рейтингу є використання TF-IDF (*частота терміна, обернена до частоти документа*[5]), який замість того, щоб визначити, наскільки поширеним є слово в усьому масиві або навіть у цьому документі, дивиться на те, наскільки важливим є певний термін у цьому документі порівняно з рештою масивів. Отже, це дає нам змогу визначити ключові терміни для кожного документа, які можуть не збігатися з найпоширенішими термінами. Ці терміни дають нам ще один набір ключових слів, які ми можемо використати в подальшій агрегації та аналізі.

[2] Noubours S, Pritzkau A, Schade U (2013) NLP as an essential ingredient of effective OSINT frameworks. In: Military communications and information systems conference (MCC), Oct 2013. IEEE, pp 1–7

[3] Manning CD, Schütze H (1999) Foundations of statistical natural language processing, vol 999. MIT press, Cambridge

[4] Rauscher J, Swiezinski L, Riedl M, Biemann C (2013) Exploring cities in crime: significant concordance and co-occurrence in quantitative literary analysis. In: Proceedings of the computational linguistics for literature workshop at NAACL-HLT, June 2013

[5] Salton G, McGill MJ (1986) Introduction to modern information retrieval

правоохоронним органом, вона опублікувала деякі зі своїх методів визначення надійності та достовірності певної інформації[32]. Вони використовують шестибальну шкалу надійності, за якою дані оцінюються від достовірних до недостовірних. Схожа, але восьмибальна шкала достовірності використовується для оцінки достовірності, рухаючись від *«підтверджено»* (*«підтверджено іншими незалежними джерелами; логічно саме по собі; узгоджується з іншою інформацією на цю тему»*), *«ймовірно»*, *«можливо»*, *«сумнівно»*, *«неймовірно»*, *«дезінформація»* (ненавмисно неправдива), *«обман»* (навмисно неправдива) і *«не можна судити про це»*. Ці питання можуть стати дуже важливими, якщо матеріал буде використовуватися як доказ у кримінальному провадженні.

НАТО також має подібну систему оцінювання надійності і достовірності з використанням шестибальної шкали для кожного з них. А фахівці рекомендують додатковий критерій оцінки до цієї шкали – оцінку довіри, згідно з якою рейтинги надійності та достовірності мають довірчий інтервал між високим, середнім та низьким рівнями[33].

Крім того, найбільш поширеною в правоохоронній системі є система 5x5x5, яка також використовує оціночні шкали щодо походження інформації[34]. Загалом, система 5x5x5 – стандартизована модель, яка включає три п'ятибальні шкали: надійність джерела, достовірність інформації та рівень доступу.

Окрім своїх рейтингових шкал, НАТО[35] також опубліковано набір контрольних списків для оцінки джерел для низки веб-джерел у сфері адвокатури, бізнесу та маркетингу, новин, інформації та особистої інформації. Ці контрольні списки заохочують аналітиків розвідувальних даних з відкритих джерел ретельно перевіряти авторитетність, точність, об'єктивність, актуальність і охоплення веб-сторінки, беручи до уваги такі критерії, як хто несе відповідальність за зміст, використовуючи граматичні перевірки як додаткову міру точності, визначаючи цілі створення такого сайту або статті, дивлячись на дату публікації сторінки і наскільки об'ємним є вміст, що міститься на ній.

Методи визначення підтвердження

Інший метод визначення достовірності полягає у використанні підтвердження: чим більше джерел роблять однакові твердження, тим більша ймовірність того, що ці твердження відповідають дійсності. Наприклад, чим більше є свідків інциденту, які погоджуються з причинами, діями та результатами, тим більшою є впевненість щодо достовірної картини події, що насправді сталася. Те ж саме можна сказати і про OSINT: чим більше відкритих джерел можливо знайти для перевірки розвідувальних даних, тим вони надійніші – хоча, може мати місце і додаткова обережність.

OSINT має два потенційних недоліки: По-перше, це ефект *«відлуння»*[36], коли джерело здається дуже достовірним через те, що існує багато джерел інформації, які пропонують ту саму інформацію; проте всі ці повідомлення базуються на одному і тому ж першоджерелі, і тому підтвердження здається вищим, ніж воно є насправді.

> *Ефект «відлуння»* – явище, коли одна й та сама інформація повторюється у багатьох джерелах, створюючи ілюзію підтвердження, хоча всі посилання ведуть до одного першоджерела. Важливо враховувати при перевірці достовірності OSINT.

По-друге, дезінформація (яка не обов'язково є навмисно неправдивою) має

[32] Department of the Army (2012) Open source intelligence. http://fas.org/irp/doddir/army/atp2-22-9. pdf

[33] Abbott C (n.d.) RC(C) evaluation system. Open briefing. http://www.openbriefing.org/ intelligenceunit/intelligencemethod/rccsystem/

[34] College of Policing (2015) Intelligence report. In: Authorised professional practice. https://www. app.college.police.uk/app-content/intelligencemanagement/ intelligence-report/

[35] NATO (2002) Exploitation of intelligence on the internet. http://www.oss.net/dynamaster/file_ archive/030201/1c0160cde7302e1c718edb08884ca7d7/Intelligence Exploitation of the Internet FINAL 18NOV02.pdf

[36] Best Jr RA, Cumming A (2007) Open source intelligence (OSINT): issues for congress, vol 5, Dec 2007

тенденцію дуже швидко поширюватися, особливо в соціальних мережах.

Таким чином, при визначенні методів підтвердження також потрібно брати до уваги перевірку джерел, що підтверджують інформацію. Іноді підтвердження може бути побічним продуктом інших методів, що використовуються для аналізу даних. Наприклад, згадані вище методи кластеризації та формального концептуального аналізу природним чином групують схожі дані, а отже, чим більша група, тим вищим буде рівень її підтвердження.

ВИСНОВОК

У сучасному інформаційному середовищі, насиченому даними з відкритих джерел, ефективне перетворення інформації на розвідувальні продукти вимагає не лише технічної спроможності, а й методологічної чіткості. Саме тому було розглянуто ключові моделі аналізу та перевірки OSINT, які забезпечують достовірну інтерпретацію багатоканальних даних. Від текстової аналітики (мішок слів, TF-IDF, конкорданс) до мережевого аналізу, геокодування, кластеризації та формального концептуального аналізу – кожен метод має свою роль у побудові цілісної картини подій, зв'язків і ризиків.

Особливу увагу приділено верифікації та оцінці достовірності, що є критично важливими для прийняття рішень у сферах безпеки, правозастосування та стратегічної комунікації. Визначення авторитетності джерел, аналіз повторюваності інформації, виявлення ефекту *«відлуння»* та застосування стандартизованих шкал (5x5x5, NATO) дозволяють підвищити надійність OSINT-продуктів.

Таким чином, моделі аналізу та перевірки OSINT не є ізольованими технічними інструментами – вони формують інтегровану аналітичну екосистему, здатну адаптуватися до складних викликів гібридної війни, кіберзагроз і дезінформації. Їхнє застосування в українському контексті – від кібербезпеки до гуманітарного моніторингу – підтверджує актуальність і стратегічну цінність багатоканальної аналітики як основи для достовірної інтерпретації відкритих даних.

РОЗДІЛ 8

ЕТИЧНІ НОРМИ ТА ЮРИДИЧНІ АСПЕКТИ ВИКОРИСТАННЯ OSINT

Наталія СВИРИДЮК
Наталія ЦЮПРИК

Експоненційне зростання цифрових загроз, терористичних атак і транснаціональної злочинності поставило демократичні суспільства перед складним вибором: як забезпечити безпеку, не порушуючи фундаментальні права людини. У цьому контексті розвідка з відкритих джерел (OSINT) стала потужним інструментом для правоохоронних органів, але її використання супроводжується низкою етичних, юридичних і соціальних викликів. Відсутність прозорості щодо алгоритмів, обсягів збору даних і меж допустимого спостереження породжує недовіру, а іноді й протест з боку громадськості, правозахисних організацій та політичних опонентів.

Сучасна практика OSINT часто балансує між законною метою захисту суспільства і ризиком порушення приватності, особливо коли йдеться про обробку персональних даних, використання фейкових профілів або тривалий моніторинг соціальних мереж. Відсутність чітких законодавчих рамок, застарілі нормативні

акти та неоднозначна судова практика створюють правову невизначеність, яка може поставити під загрозу легітимність зібраних доказів і саму репутацію правоохоронних органів.

Паралельно з цим, зростає потреба у міждержавній координації, стандартизації процедур і впровадженні принципів, які дозволяють інтегрувати захист даних у саму архітектуру OSINT-інструментів. Глобальні інституції, такі як Європол, Інтерпол та Євроюст, відіграють ключову роль у формуванні спільного підходу до боротьби з кіберзлочинністю, але національні відмінності в законодавстві залишаються серйозною перешкодою.

Публічна думка, особливо після викриттів масового стеження, стала важливим фактором, що впливає на політику безпеки. Саме тому критично важливо забезпечити прозорість, підзвітність і освітню роботу щодо можливостей, обмежень та етичних стандартів OSINT. Лише за таких умов можна досягти балансу між ефективністю цифрових розслідувань і збереженням демократичних цінностей.

Для України дослідження етичних і юридичних аспектів OSINT має особливе значення в контексті євроінтеграційних процесів. Вивчення досвіду європейських країн – зокрема Великої Британії, яка демонструє високий рівень нормативної деталізації, прозорості та публічного контролю – дозволяє адаптувати найкращі практики до національного контексту, не втрачаючи при цьому зв'язку з фундаментальними принципами правової держави. Такий підхід сприяє формуванню довіри до правоохоронних органів, забезпечує легітимність цифрових розслідувань і закладає основу для створення етично стійкої, технологічно компетентної системи кібербезпеки, сумісної з європейськими стандартами.

Після терактів 11 вересня більша частина західного демократичного світу дедалі більше намагається знайти баланс між традиційними ліберальними цінностями та сучасними проблемами безпеки[1]. У світлі міжнародних терористичних атак, кількість яких зросла в п'ять разів з 2000 року[2], а також атак у Брюсселі, Парижі та Тунісі, з'явилися повідомлення, що уряди дедалі частіше підштовхують технології спостереження та розслідування до нових прецедентів[3]. Хоча уряд захищає таку політику сек'юритизації як необхідну, вона все частіше зустрічається з критикою як з боку опозиційних партій, так і з боку громадськості, політичних активістів і навіть неурядових організацій, таких як *«Міжнародна амністія»* (**Amnesty International**). Хоча таке занепокоєння викликане насамперед тероризмом, додаткову критику викликала нещодавня невизначеність потенційного внутрішнього екстремізму та серйозні кримінальні прояви[4], які потрапляють під нагляд. Часто ЗМІ та групи активістів називають такі підходи загальною *«масовою істерією»* щодо недоречного та невиправданого профілювання[5].

Загалом, можливим є виділення трьох критичних наративів, які впливають на громадську, політичну та поліцейську сферу OSINT епохи Інтернету: відсутність ясності в суспільстві щодо теми OSINT; протилежні наративи та контрдиктаторські аргументи, висунуті проти легітимності та пропорційності; і розглядається інформація та твердження з незалежних і загальнодоступних оглядів, що стосуються практики OSINT.

Випадок Великої Британії заслуговує на увагу широкої аудиторії. Трагічна тенденція до зростання кількості терористичних атак і жертв, а також постійні руйнування, переміщення і дезорганізація в різних частинах Близького Сходу

[1] Moss K (2011) Balancing liberty and security: human rights, human wrongs. Springer, Berlin

[2] Institute for Economics and Peace (2014) Global Terrorism Index 2014: measuring and understanding the impact of terrorism

[3] Elworthy S (2015) Beyond deterrence: rethinking UK Security Doctrine | Oxford Research Group. Retrieved 20 July 2016. http://www.oxfordresearchgroup.org.uk/publications/ briefing_papers_and_reports/beyond_deterrence_rethinking_uk_security_doctrine

[4] Jones J (2015) The day I found out I'm a 'Domestic Extremist'. The Telegraph. http://www.telegraph.co.uk/news/uknews/terrorism-in-theuk/11357175/The-day-I-found-out-Im-a-Domestic-Extremist.html

[5] Evans R, Bowcott O (2014) Green Party peer put on database of 'extremists' after police surveillance. The Guardian. http://www.theguardian.com/politics/2014/ jun/15/green-party-peer-put-on-database-of-extremists-by-police

призвели до того, що багато країн ЄС стали перед необхідністю посилення безпеки і спостереження, зокрема, для боротьби з тероризмом, імміграцією та організованою злочинністю. Таким чином, будучи однією з найбільш географічно безпечних і ретельно контрольованих країн Європи[6], Велика Британія є чудовим прикладом для наслідування, оскільки широка європейська аудиторія може наслідувати її приклад, якщо тенденції продовжуватимуться і надалі. Дійсно, щодо насильницької радикалізації такі країни, як Іспанія, Франція, Бельгія і Німеччина, посилили заходи безпеки і спостереження[7]. Навіть тимчасове посилення безпеки може викликати значний суспільний резонанс, тому врахування наслідків британського OSINT і спостереження є важливою умовою для забезпечення стійкості і безперервності діяльності.

ВІДСУТНІСТЬ ЯСНОСТІ В СУСПІЛЬСТВІ ЩОДО ТЕМИ OSINT

Незважаючи на стрімкий розвиток інструментів OSINT та їхнє впровадження у сферу безпеки, суспільне розуміння цієї практики залишається фрагментарним і часто спотвореним. Відсутність чіткої інформації про принципи роботи, межі повноважень та правові рамки використання розвідкою відкритих джерел породжує недовіру, підозри та спекуляції. Особливо це актуально в умовах, коли цифрові рішення, що використовуються правоохоронними органами, залишаються закритими для громадського контролю, а їхні алгоритми непрозорими.

У публічному дискурсі OSINT нерідко асоціюється з масовим стеженням, що посилюється прикладами з міжнародної практики. Це створює ризик ототожнення OSINT із порушенням приватності, навіть коли йдеться про законні та етично обґрунтовані розслідування. Водночас, недостатня комунікація з боку державних інституцій щодо цілей, методів і обмежень OSINT лише поглиблює розрив між фаховою практикою і громадським сприйняттям.

Для України, яка прагне інтегруватися в європейський правовий простір, критично важливо не лише впроваджувати технології OSINT, а й забезпечити їхню легітимність через прозорість, публічну освіту та дотримання принципів демократичного контролю. Вивчення досвіду Великої Британії, країни з високим рівнем нормативної деталізації та публічного обговорення цифрових повноважень, може стати орієнтиром для формування збалансованої моделі, де безпека не суперечить свободі, а технології служать суспільному добру.

З огляду на постійні дебати про безпеку і свободу між політичними групами, а також представниками громадськості та чинним урядом, можна припустити, що відносно сучасна інтеграція інтернет-можливостей OSINT для спостереження і розслідування значно перебільшена (наприклад, витоки Сноудена, які більше стосуються секретних служб) або неправильно зрозуміла з точки зору фактичної практики і правових рамок, в яких вони діють[8]. Наприклад, одна з таких варіацій програмного забезпечення OSINT, що використовується різними правоохоронними органами, *«COSAIN»*, є значною мірою секретною філією **Capita**[9], яку купила компанія *«Barrachd Ltd»*, компанія з розробки рішень для великих даних, що базується в Единбурзі, Великобританія. COSAIN має дуже обмежену інформацію у відкритому доступі[10], не має офіційного веб-сайту і не може бути розміщена в домені веб-сайту **Barrachd Ltd**. Хоча це не означає, що інформація обов'язково є суперечливою, недостатня прозорість може підірвати відносини між поліцією та громадськістю, посилити підозри, недовіру та

[6] Barrett D (2013) One surveillance camera for every 11 people in Britain, says CCTV survey. The Telegraph http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html

[7] Ryan M (2016) Brussels attacks rekindle privacy vs. security debate in Europe. Washington post. https://www.washingtonpost.com/world/europe/brusselsattacks-rekindle-privacy-vs-security-debate-in-europe/2016/03/26/60a68558-f2dc-11e5-a2a3-d4e9697917d1_story.html.

[8] Carey HP (2015) Managing 'Threats': uses of social media for policing domestic extremism and disorder in the UK

[9] Cameron G (2015) Capita buys Scottish analytics firm Barrachd (From Herald Scotland). http://www.heraldscotland.com/business/13416378.Capita_buys_Scottish_analytics_firm_Barrachd/

[10] Cosain E (2015) Barrachd Edinburgh, UK. http://assets-production.govstore.service.gov.uk/G4/Barrachd-0879/523c2390354067df0ce14172/QD5/13_0125_BAR_Cosain_A4_ flyer.pdf

ВИСНОВОК

Загалом, необхідно вивчити суб'єктивні наративи різних сторін, які можуть бути чутливими до сучасної практики OSINT або потенційно виступати проти неї. Усвідомлення постійних протиріч між такими школами думки необхідне для мінімізації негативної уваги, яка може завдати шкоди репутації та ресурсам фахівців-практиків.

Потрібно оцінити сучасні виклики та перспективи, що оточують сферу розслідувань та спостереження за допомогою відкритих джерел розвідки. Громадська, приватна та державна думка на цю тему значною мірою є впливовою та авторитетною щодо OSINT через вкрай скептичну та обережну суспільно-політичну позицію. Тому в спільних інтересах практиків OSINT, зацікавлених сторін у сфері безпеки, а також представників громадськості та уряду, потрібно забезпечити максимальну прозорість, обізнаність і освіту щодо тих аспектів боротьби з OSINT, які вимагають розсудливості, таких як конкретні інструменти, програми і тактики. Тим не менш, фахівці з OSINT повинні докладати зусиль для подальшої публікації обмежень своїх можливостей, якщо це можливо, щоб заспокоїти громадськість, а також чітко документувати і публікувати пропорційні обґрунтування і дозволи, які дозволяють застосовувати OSINT. Дійсно, відсутність фізичної присутності поліції, за якою могла б спостерігати і контролювати громадськість, може викликати занепокоєння у деяких людей. Тому слід з розумною відданістю поширювати через практиків OSINT обмежувальні вказівки законодавства, а також інформацію щодо захисту даних, стандартів моніторингу та ведення журналів. Подібно до того, як широка громадськість, ЗМІ та приватна сфера відчувають себе одночасно захищеними від правоохоронних органів завдяки загальній обізнаності про обсяг і обмеження поліцейських повноважень, цифровий спектр поліцейської діяльності також потребує більш чіткого визначення процедур і обмежень OSINT в Інтернеті, щоб заспокоїти експертів, які не є фахівцями в цій галузі, і уникнути потенційних суперечок і невдоволення.

Загалом, використовуючи приклад Сполученого Королівства як приклад суспільства з високим рівнем спостереження і моніторингу безпеки, фахівці-практики можуть передбачити потенційні сценарії, в яких державні, приватні, медійні, опозиційні та політичні наративи можуть створювати проблеми, бар'єри і можливості для дискусій щодо розслідувань OSINT-атак. Зокрема, важливо звернути увагу на такі приклади, як публічна доступність юридичних документів та незалежні огляди OSINT-розслідувань, оскільки подібні процеси відбуваються по всій Європі. Саме завдяки відкритому поширенню таких матеріалів можна краще розвіяти наративи дезінформації та неправдивих відомостей.

Більшість правових питань випливають з міркувань прав людини. Окрім національних, європейських та міжнародних документів, які безпосередньо захищають основні права і свободи, закони про захист даних ґрунтуються на ЄКПЛ і тісно пов'язані з правом на недоторканність приватного життя. Аналогічно, закони, що регулюють питання доказів і розкриття інформації, спрямовані на реалізацію та захист права на справедливий судовий розгляд і запобігання судовим помилкам.

Громадська думка є важливим фактором, який слід враховувати; хоча це і не є правовим питанням, те, як діяльність поліції сприймається в загальному масштабі, може мати величезний вплив.

Можливо, ми живемо в цифрову епоху, коли люди живуть своїм життям і вчиняють злочини в кіберсередовищі, але ніколи ще люди не були настільки об'єднані в глобальному масштабі, щоб вимагати захисту своїх прав людини. Ми можемо відрізняти кіберзлочинність від традиційної злочинності, але по суті все зводиться до того, що реальні люди завдають шкоди або збитків іншим

реальним людям, і з цим пов'язані правові питання.

Хоча ця сфера розвивається настільки стрімко, що відповідне законодавство не встигає за нею, розробляються і впроваджуються нові закони, які сприяють спільній роботі, допомагають визначити обсяг і характер повноважень поліції, а також враховують умовні права людини і визначають прийнятний ступінь втручання в обмін на посилення безпеки і захисту в Інтернеті. Саме такого балансу прав необхідно досягти і підтримувати, і саме він повинен лежати в основі всіх розслідувань.

РОЗДІЛ 9

ПЕРСПЕКТИВИ ОБ'ЄДНАННЯ ТА ІНТЕГРАЦІЇ OSINT ІНСТРУМЕНТІВ ДО НАЯВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Юрій КРУТІК
Роман РАСКЕВИЧ

У сучасних умовах стрімкого розвитку інформаційних технологій, зростання відкритих джерел даних та активізації гібридних загроз, правоохоронні органи України стикаються з необхідністю підвищення ефективності аналізу відкритої інформації. Одним із перспективних напрямів удосконалення діяльності в цій сфері є інтеграція інструментів OSINT (Open Source Intelligence) до наявних інформаційно-аналітичних систем. Це дозволяє забезпечити оперативний доступ до релевантної інформації, автоматизувати процеси збору, обробки та візуалізації даних, а також покращити ухвалення рішень у сфері національної безпеки. У сучасних умовах, коли ефективність рішень залежить від швидкості доступу до достовірних даних, інтеграція інструментів відкритої розвідки в наявні інформаційні системи стає не просто технологічним оновленням, а стратегічною потребою.

Фрагментованість цифрових платформ, дублювання функцій, обмежений обмін між відомствами та відсутність єдиних стандартів обробки даних суттєво знижують потенціал аналітичних підрозділів. Водночас, міжнародний досвід демонструє, що саме централізована інтеграція OSINT-модулів – через API, мікросервісну архітектуру, брокери повідомлень – дозволяє забезпечити масштабованість, гнучкість і ситуаційну обізнаність у реальному часі. Для України, яка перебуває в умовах повномасштабної війни, така інтеграція є критично важливою для виявлення загроз, ідентифікації об'єктів оперативного інтересу, прогнозування ризиків та підтримки управлінських рішень на всіх рівнях.

Системне впровадження OSINT у державні інформаційні системи має спиратися не лише на технічні рішення, а й на нормативне врегулювання, уніфікацію підходів, розвиток компетенцій персоналу та забезпечення кіберстійкості. Це дозволить перетворити відкриту інформацію з розрізненого ресурсу на стратегічний актив, здатний посилити національну безпеку, правопорядок і довіру до державних інституцій.

В умовах активної протидії збройній агресії рф, правоохоронному та оборонному секторам необхідний доступ до інформації, як з державних реєстрів так і відкритих інтернет ресурсів з метою ефективної протидії агресії, розслідування злочинів та підтримання правопорядку.

Державними органами, які використовують інструменти та методи OSINT

Все це інтегроване на рівні бекенду державної платформи, а не використовується вручну.

FBI Sentinel + OSINT Connectors.

FBI використовує системи, які інтегрують відкриті джерела у кейси, наприклад:

- автоматичне прикріплення матеріалів з YouTube, Telegram;
- прив'язка геолокацій до публічних джерел (Wikimapia, OpenStreetMap).

4. **Велика Британія***: OSINT-модулі в системах контртерору*

PREVENT / Home Office Intelligence Platform.

Інтегровано OSINT-системи, що збирають, класифікують і архівують контент з відкритих джерел, зокрема:

- відео- та фото-контент із соцмереж;
- форуми, Telegram-канали;
- коментарі, індикатори радикалізації.

Усе це безпосередньо вбудовано у державну інформаційну систему, не як зовнішній інструмент.

ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ

Інтеграція OSINT-інструментів до систем правоохоронних органів потребує нормативного врегулювання. Зокрема, мають бути визначені:

- правила використання відкритих джерел інформації;
- критерії достовірності та допустимості таких даних у процесах розслідування;
- регламенти щодо захисту персональних даних;
- моделі атестації безпеки зовнішніх компонентів.

Ідеальним варіантом слугує розроблення національних методичних підходів до впровадження OSINT у діяльність державних органів, з урахуванням кращих світових практик.

ВИСНОВКИ

Інтеграція OSINT-інструментів у державні інформаційні системи України є не лише технологічним викликом, а стратегічною необхідністю в умовах сучасної безпекової реальності. Вона дозволяє трансформувати фрагментовану цифрову інфраструктуру в єдину, адаптивну екосистему, здатну оперативно реагувати на загрози, виявляти приховані зв'язки та підтримувати обґрунтовані управлінські рішення. Успішне впровадження таких рішень потребує комплексного підходу: поєднання технічної архітектури, нормативного регулювання, захисту даних, а також розвитку компетентностей персоналу.

Міжнародний досвід підтверджує ефективність OSINT як інструменту державної аналітики, коли він інтегрований не як зовнішній додаток, а як бекендова складова національних платформ. Для України це означає перехід від ручного використання відкритих джерел до автоматизованої, стандартизованої та безпечної роботи з ними, у межах єдиної платформи, яка об'єднує правоохоронний та оборонний сектори. Такий підхід не лише підвищує якість рішень, а й сприяє економії ресурсів, зміцненню кіберстійкості та формуванню нової культури аналітики, заснованої на прозорості, етичності та міжвідомчій взаємодії.

Системне впровадження OSINT – це інвестиція в національну безпеку, довіру до державних інституцій та здатність України діяти на випередження в умовах постійно змінюваного інформаційного середовища.

РОЗДІЛ 10

АВТОМАТИЗАЦІЯ АНАЛІТИЧНИХ БІЗНЕС-ПРОЦЕСІВ ЧЕРЕЗ СМАРТ-КОНТРАКТИ: НОВІ МОЖЛИВОСТІ ТОКЕНІЗАЦІЇ В РОЗВІДУВАЛЬНІЙ АНАЛІТИЦІ

Денис ПЕФТІЄВ

В умовах сучасного світу інформація вже набула статусу стратегічного ресурсу, що визначає не лише успіхи окремих бізнес-структур, а й глобальну безпеку та стабільність соціально-економічних систем[1]. Проте, незважаючи на стрімкий розвиток технологій збору та обробки інформації, галузь аналітики даних залишається обмеженою низкою системних проблем, які значно стримують її еволюцію[2]. Зокрема, сучасні аналітичні процеси, особливо в критично важливих сферах як безпека та аналітична розвідка, зазнають негативного впливу через фрагментарність джерел та складність верифікації достовірності інформації[3]. Аналітики змушені витрачати значний ресурс часу на перевірку даних та ручну обробку інформації, що призводить до затримок у прийнятті управлінських рішень та втрати актуальності даних, що є критичним для OSINT[4].

Окремої уваги заслуговує фундаментальний виклик, пов'язаний із централізованою моделлю управління знаннями (результатами аналітичних досліджень), за якої контроль належить окремим великим провайдерам, що унеможливлює створення гнучких, децентралізованих систем та призводить до монополізації ринку даних[5].

Крім цього, на сьогоднішній день відсутня прозора система збору, зберігання та використання даних в рамках розвідувальної аналітики, а також відсутня еволюційна модель розвитку цієї системи. Це означає, що нерідко при зміні керівництва профільного підрозділу застосовується політика *«чистого аркушу»* (*«табула раса»*), суть якої полягає в тому, що нова команда повністю ігнорує попередній досвід, створює все *«з нуля»*, проте по факту створюють системи або ініціативи, які фактично повторюють старі – але без визнання спадкоємності.

Однією з найбільш перспективних відповідей на зазначені виклики визначено інтеграцію технологій Web3, насамперед, смарт-контрактів і моделей децентралізованих автономних організацій (DAO), у сферу аналітики даних[6]. Смарт-контракти, як самовиконувані програмні конструкції, дають змогу автоматизувати значну частину бізнес-процесів перевірки та поширення даних, забезпечуючи незмінність умов та прозорість транзакцій (і як наслідок процесів аналітичної діяльності)[7]. Водночас DAO створюють інституційну базу для формування спільнот, які управляють обігом знань та проводять верифікацію інформації, формуючи peer-to-peer економіку даних[8].

---

[1] Tapscott D., Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin, 2016; Swan M. Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015.

[2] Zhang Y. et al. The challenges and countermeasures of blockchain in finance and banking. Journal of Computer Information Systems, 2019.

[3] World Economic Forum. The Global Risks Report 2019. URL: https://www.weforum.org/reports/the-global-risks-report-2019/ (дата звернення: 14.07.2025).

[4] Buterin V. A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum White Paper, 2014. URL: https://ethereum.org/en/whitepaper/ (дата звернення: 14.07.2025).

[5] Feeney M. K. Making (and remaking) the rules: The role of institutional entrepreneurs in the evolution of information policy. The Information Society, 2018; European Parliament. Resolution on distributed ledger technologies and blockchains: building trust with disintermediation. 2018. URL: https://www.europarl.europa.eu/doceo/document/TA-8-2018-0373_EN.html (дата звернення: 14.07.2025).

[6] Mougayar W. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley, 2016.

[7] Luu L. et al. Making Smart Contracts Smarter. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016; Atzei N., Bartoletti M., Cimoli T. A Survey of Attacks on Ethereum Smart Contracts (SoK). Principles of Security and Trust, 2017; ConsenSys. Ethereum Smart Contract Best Practices. URL: https://consensys.github.io/smart-contract-best-practices/ (дата звернення: 14.07.2025).

[8] Aragon. Aragon Whitepaper. 2017. URL: https://aragon.org/whitepaper.pdf (дата звернення: 14.07.2025); DAOstack. DAOstack Whitepaper. 2018. URL: https://docs.google.com/document/d/1_s_I2u3x-mLn_5a_f-22Yxbezx5rW4c2P1wHnaZmwKA/edit (дата звернення: 14.07.2025); Chen Y., Bellavitis C. Blockchain's Disruption of the E-commerce Platform. Journal of Strategic Information Systems, 2020.

ТЕОРЕТИКО-ТЕХНОЛОГІЧНІ ОСНОВИ

Актуальність застосування смарт-контрактів в аналітиці

На сучасному етапі смарт-контракти вийшли далеко за межі концепції виключно фінансових транзакцій та стали універсальним інструментом автоматизації бізнес-процесів, у тому числі в галузі аналітики даних[9]. Відповідно до визначення[10], смарт-контракт є програмою, що самостійно виконується за умови дотримання заданих параметрів, що усуває необхідність довіри до третіх сторін[11]. У сфері аналітики даних виникає можливість автоматизувати ключові етапи роботи, серед яких: валідація джерел, логіка дистрибуції інформації, розрахунок винагород для аналітиків та моніторинг змін у ризикових профілях[12].

Критично важливою перевагою смарт-контрактів є їх незмінність після розгортання в блокчейні[13]. Це є вирішальним для безпеки аналітичних процесів, де будь-яке порушення логіки може призвести до фальсифікації інформації[14] і як наслідок втрати довіри до самого аналітичного продукту. Для розробки смарт-контрактів використовуються різні мови програмування, зокрема Solidity (Ethereum), Vyper, CosmWasm (Rust), Ink! (Substrate) та Move (Aptos, Sui), які забезпечують різні рівні безпеки та ефективності[15]. Наприклад, застосування CosmWasm дозволяє створювати смарт-контракти на мові Rust, що підвищує безпеку коду завдяки сильній типізації[16].

З метою уникнення типових вразливостей (Reentrancy атаки, Integer Overflow/Underflow тощо) впроваджено стандарти безпеки та бібліотеки перевірених шаблонів коду, як-от OpenZeppelin Contracts та ConsenSys Best Practices[17]. Історія гучних зламів, наприклад кейс The DAO (2016), підтверджує критичну важливість дотримання зазначених стандартів[18]. Таким чином, для аналітичних DAO смарт-контракти виступають технічним ядром, на якому будується довіра до даних, прозорість взаємодій і автоматизація процесів.

Огляд сучасних блокчейн-платформ для DAO-аналітики

В останні роки ландшафт блокчейн-платформ, придатних для реалізації DAO-аналітики, зазнав фундаментальних змін. Якщо раніше Ethereum практично монополізував ринок[19], то наразі ситуація виглядає набагато багатовекторнішою з огляду на вартість користування та технологічні інновації[20].

Ethereum та Layer 2-рішення. Протягом тривалого часу ключовою проблемою Ethereum залишалися високі комісії (Gas Fees), що робило його використання для великої кількості транзакцій, які є частиною автоматизації процесів, економічно недоцільним[21]. Однак ситуація суттєво змінилася із запровадженням Ethereum Layer 2-рішень (Arbitrum, Optimism) та переходом на Proof-of-Stake, що дозволило

[9] European Parliament. Resolution on distributed ledger technologies and blockchains: building trust with disintermediation. 2018. URL: https://www.europarl.europa.eu/doceo/document/TA-8-2018-0373_EN.html (дата звернення: 14.07.2025)..

[10] Buterin V. A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum White Paper, 2014. URL: https://ethereum.org/en/whitepaper/ (дата звернення: 14.07.2025).

[11] Atzei N., Bartoletti M., Cimoli T. A Survey of Attacks on Ethereum Smart Contracts (SoK). Principles of Security and Trust, 2017.

[12] Luu L. et al. Making Smart Contracts Smarter. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016; ConsenSys. Ethereum Smart Contract Best Practices. URL: https://consensys.github.io/smart-contract-best-practices/ (дата звернення: 14.07.2025).

[13] Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper, 2014.

[14] Atzei N., Bartoletti M., Cimoli T. A Survey of Attacks on Ethereum Smart Contracts (SoK). Principles of Security and Trust, 2017.

[15] Dannen C. Introducing Ethereum and Solidity. Apress, 2017; Liskov B. The Power of Abstraction. Communications of the ACM, 2018.

[16] CosmWasm Docs. Official Documentation. URL: https://docs.cosmwasm.com (дата звернення: 14.07.2025).

[17] ConsenSys. Ethereum Smart Contract Best Practices. URL: https://consensys.github.io/smart-contract-best-practices/ (дата звернення: 14.07.2025); OpenZeppelin Contracts. Library for secure smart contract development. URL: https://openzeppelin.com/contracts/ (дата звернення: 14.07.2025).

[18] Atzei N., Bartoletti M., Cimoli T. A Survey of Attacks on Ethereum Smart Contracts (SoK). Principles of Security and Trust, 2017; ConsenSys. Ethereum Smart Contract Best Practices. URL: https://consensys.github.io/smart-contract-best-practices/ (дата звернення: 14.07.2025).

[19] Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper, 2014.

[20] Mougayar W. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley, 2016.

[21] Binance Research. The State of the Blockchain Industry. 2019; CoinDesk Research. Quarterly Review. 2021.

ВИКЛИКИ І ПЕРСПЕКТИВИ DAO-АНАЛІТИКИ В КОНТЕКСТІ OSINT

Застосування DAO-аналітики для потреб OSINT відкриває нові горизонти автоматизації, прозорості та децентралізації розвідувальної діяльності. Водночас, ця модель стикається з низкою технологічних, організаційних та нормативних викликів, які потребують системного вирішення.

- **Інфраструктурна масштабованість**. DAO-системи, що працюють на публічних блокчейнах, можуть бути перевантажені великою кількістю транзакцій, що ускладнює оперативну обробку OSINT-запитів. Для вирішення цієї проблеми доцільно використовувати Layer 2-рішення, сайдчейни або гібридні моделі з частковим винесенням обчислень поза блокчейн.
- **Операційна продуктивність**. У великих DAO-структурах, що обробляють OSINT-дані, виникає ризик фрагментації, дублювання запитів та затримок у валідації. Впровадження DAO-календарів, смарт-делегування голосів та автоматичне ранжування запитів може забезпечити стабільність і ефективність процесів.
- **Залежність від зовнішніх джерел**. Смарт-контракти не мають прямого доступу до реального світу, що обмежує їхню здатність реагувати на динамічні OSINT-події. Інтеграція Oracle-сервісів (наприклад, Chainlink) дозволяє отримувати санкційні списки, судові рішення та інші критично важливі дані в режимі реального часу.
- **Юридична невизначеність**. DAO-аналітика в OSINT-контексті потребує відповідності міжнародним нормам (GDPR, FATF) та адаптації до українського законодавства. Впровадження моделей *«анонімного KYC»*, знеособлених звітів і гібридних форм реєстрації (наприклад, ГО з DAO-протоколами) може забезпечити легітимність і правову стійкість.
- **Відповідальність за аналітичні продукти**. У DAO-моделі виникає питання колективної відповідальності за достовірність OSINT-звітів. Відсутність централізованого контролю вимагає впровадження репутаційних механізмів, peer-review та системи штрафів за поширення недостовірної інформації.
- **Перспективи розвитку**. DAO-аналітика здатна трансформувати OSINT у відкриту, динамічну екосистему, де аналітики з різних регіонів можуть спільно формувати звіти, перевіряти джерела та монетизувати дані через токенізовані ринки. Це відкриває шлях до створення Data Mining DAO — нової форми економіки даних, де OSINT стає не лише інструментом безпеки, а й стратегічним активом.

ВИСНОВОК

DAO-аналітика, побудована на основі смарт-контрактів, токенізації та децентралізованого управління, пропонує радикально нову модель організації аналітичної діяльності – прозору, масштабовану, стійку до маніпуляцій і здатну до самоадаптації. У контексті OSINT ця модель дозволяє автоматизувати ключові етапи збору, валідації та поширення відкритих даних, забезпечуючи швидкість, достовірність і довіру до аналітичного продукту.

Для України, яка перебуває в умовах гібридної війни, системне впровадження DAO-аналітики є не просто технологічним оновленням, а стратегічним кроком до побудови нової архітектури безпеки. Це дає змогу створити динамічну екосистему OSINT, де кожен учасник – аналітик, верифікатор, замовник – діє в умовах прозорих правил, автоматизованих процесів і репутаційної відповідальності.

Інституалізація DAO-аналітики в Україні потребує нормативної підтримки, технічної інфраструктури, освітніх програм і міжвідомчої координації. Але її потенціал – у здатності перетворити розрізнені дані на стратегічну перевагу, а аналітичну діяльність – на інструмент довіри, стійкості та проактивного управління ризиками.

"*Аналітика як культура: між даними, сенсом і дією*" -
Авторська формула

«Інновація – це коли знання стає дією, а дія – культурою» (Пітер Друкер), і в цьому процесі *«Штучний інтелект – це не заміна людського розуму, а його дзеркало. І ми самі вирішуємо, що в ньому побачити»* (Фей-Фей Лі). У контексті OSINT штучний інтелект виконує функцію когнітивного розширення, а не заміщення людського аналізу. Це визначає необхідність критичного осмислення алгоритмічних результатів та їх інтеграції в гуманітарно орієнтовані аналітичні моделі.

Українські підходи до OSINT не базуються на реплікації зовнішніх практик, а на адаптивному реагуванні на нестандартні виклики, яких раніше не існувало. Це формує нову аналітичну культуру, засновану на етиці, адаптивності й стратегічному мисленні, яка поєднує технологічну інновацію з етичними та стратегічними засадами.

Ця частина монографії – не просто огляд інструментів. Це маніфест того, як технологія, етика та стратегія об'єднуються в українському OSINT, щоб не лише реагувати на загрози, а й формувати нову реальність – прозору, стійку і людяно осмислену. Ця частина – про те, як аналітика перестає бути лише інструментом і стає частиною національного характеру: етичною, адаптивною, стратегічною.

ВІТЧИЗНЯНІ ІННОВАЦІЇ В OSINT

ЧАСТИНА ІІІ

РОЗДІЛ 11

СЕМАНТИЧНИЙ НЕТВОРКІНГ В ЗАДАЧАХ OSINT

Дмитро ЛАНДЕ

Семантичний нетворкінг – науково-методологічна парадигма, спрямована на автоматизоване формування, аналіз та модифікацію семантичних мереж з використанням великих мовних моделей (LLM). Основне призначення семантичного нетворкінгу – розширення можливостей аналізу даних за рахунок інтеграції методів штучного інтелекту, семантичного моделювання та обробки природної мови. Він передбачає реалізацію концепції *«рою віртуальних експертів»*, яка базується на багаторазовому опитуванні LLM для виявлення ключових понять, встановлення їхніх взаємозв'язків, оцінки значущості цих зв'язків та генерації нових знань на основі наявної інформації.

Такий підхід дозволяє не лише автоматизувати процес побудови складних семантичних структур, але й адаптувати їх до потреб аналітики в таких галузях, як OSINT, кібербезпека, стратегічне прогнозування та інтелектуальний аналіз даних.

СЕМАНТИЧНІ МЕРЕЖІ

Із семантичним нетворкінгом безпосередньо пов'язано поняття семантичних мереж, які виступають у ролі універсального інструменту моделювання та організації знань, особливо ефективно вони застосовуються в сфері Open Source Intelligence (OSINT). У контексті OSINT семантичні мережі забезпечують формалізоване представлення інформації, отриманої з різноманітних відкритих джерел, таких як веб-ресурси, соціальні мережі, наукові публікації чи новинні агентства. Вони дозволяють структурувати неструктуровані дані, встановлювати приховані зв'язки між об'єктами, а також інтегрувати розподілену інформацію в єдину аналітичну модель.

Семантичні мережі реалізуються у вигляді графів, де вершини представляють сутності (персонажі, події, географічні об'єкти тощо), а ребра — смислові або причиново-наслідкові відношення між ними. Ця властивість робить їх надзвичайно корисними для аналізу складних систем, побудови профілів суб'єктів, виявлення шаблонів поведінки та прогнозування подій на основі відкритих даних.

Перші кроки у використанні семантичних мереж було зроблено ще в 1956 році Річардом Річенсом[1] в рамках досліджень з машинного перекладу в Кембриджському центрі вивчення мов. У цій ранній концепції графова модель використовувалася для формалізації значень слів та смислових зв'язків між ними, що сприяло автоматизації лінгвістичних процесів. Цей підхід став основою для подальшого розвитку методів опрацювання природної мови, які нині широко використовуються в системах збирання, фільтрації та аналізу відкритих даних у рамках OSINT.

З початку 1980-х років концепція семантичних мереж набула нового розвитку разом із становленням веб-технологій. Особливого значення вона досягла в рамках ідеї Семантичного вебу, запропонованої Тімом Бернерсом-Лі[2] – творцем World Wide Web. Метою цієї ініціативи було створення середовища, в якому інформація була б доступною не лише для людського сприйняття, але й для автоматизованої обробки програмними засобами. Це стало важливим етапом у розвитку технологій, орієнтованих на інтеграцію, класифікацію та аналіз великих масивів відкритих даних, що має пряме відношення до сучасних

[1] Lehmann Fritz, Rodin Ervin Y., eds. (1992). Semantic networks in artificial intelligence. International series in modern applied mathematics and computer science. Vol. 24. Oxford; New York: Pergamon Press. ISBN 0080420125

[2] Berners-Lee T., Hendler J., Lassila O. The semantic web. Scientific American, 2001. Vol. 284, No. 5. – pp. 34-43.

практик OSINT.

Концепція Семантичного вебу, започаткована як наукова ідея Тіма Бернерса-Лі, передбачала створення такого інформаційного середовища, де дані були б не лише доступними для людського сприйняття, але й зрозумілими для автоматизованої обробки машинами. У цьому контексті веб як мережева структура отримав можливість автоматично інтегрувати дані з різноманітних джерел, ефективно локалізувати потрібну інформацію та формувати основу для побудови інтелектуальних систем. Семантичний веб охоплює широкий спектр стандартів, форматів та технологій, призначених для формального опису понять, термінів і взаємозв'язків між ними в межах конкретних предметних галузей. Це забезпечує структуроване представлення знань, що, в свою чергу, створює умови для глибшого аналізу, інтеграції та взаємодії інформації на глобальному рівні.

У рамках методології OSINT такі технології мають особливе значення, оскільки забезпечують формалізацію, семантичне узагальнення та аналіз масивів неструктурованих даних, зібраних із відкритих джерел — соціальних мереж, новинних порталів, наукових публікацій, офіційних документів тощо. Семантичні мережі дозволяють моделювати сутності (персонажі, події, місця, організації), встановлювати між ними причиново-наслідкові, часові, просторові чи інші типи зв'язків, що надзвичайно важливо для комплексного аналізу ситуацій, прогнозування розвитку подій, побудови профілів або виявлення шаблонів поведінки.

СЕМАНТИЧНИЙ НЕТВОРКІНГ ЯК НОВИЙ РІВЕНЬ СЕМАНТИЧНОГО МОДЕЛЮВАННЯ

Застосування класичних семантичних мереж має обмеження, пов'язані з високими витратами на їхнє проектування, наповнення та підтримку актуальності. Ці проблеми значною мірою подолані завдяки розвитку великих мовних моделей, які здійснили революцію в обробці текстової інформації. Інтеграція технологій штучного інтелекту, зокрема LLM, з семантичними мережами та концепціями Семантичного вебу, стала основою для появи нового рівня представлення знань — семантичного нетворкінгу.

Семантичний нетворкінг передбачає автоматизоване формування графів знань на основі аналізу текстових даних, що дозволяє не лише ефективно будувати семантичні мережі, але й адаптувати їх до складних, динамічно змінюваних інформаційних середовищ. Основою цієї технології є концепція *«рою віртуальних експертів»*, у якій LLM багаторазово обробляє текстові масиви, виділяючи ключові концепти та встановлюючи між ними смислові зв'язки через процедури агрегації та аналізу інформації. Такий підхід забезпечує не лише точність представлення знань, але й їхню гнучкість у подальших модифікаціях.

У процесі реалізації семантичного нетворкінгу здійснюється звернення до LLM з метою виявлення пар семантично пов'язаних понять у певній предметній області. Виявлені пари фіксуються та додаються до загальної мережі, що поступово розширюється. Це дає змогу формувати різні типи мереж: зважені та незважені, спрямовані та неспрямовані, кожна з яких може використовуватися залежно від аналітичної задачі.

Особливий науковий і практичний інтерес становлять причинно-наслідкові (каузальні) мережі, які дозволяють моделювати ланцюги взаємодії між подіями та сутностями. Такі мережі можуть слугувати основою для побудови аналітичних сценаріїв, що забезпечує глибше розуміння механізмів розвитку подій у досліджуваній області. Вони відкривають нові можливості для аналізу причинно-наслідкових зв'язків між елементами, що є критично важливим для прийняття обґрунтованих рішень на основі прогнозування та моделювання різних сценаріїв.

різними *«віртуальними експертами»*, що ускладнює побудову узгодженої мережі та вимагає додаткової фільтрації або агрегування. Крім того, якість результатів залежність від самих промптів, які відіграють ключову роль у *«рої віртуальних експертів»*, і якість відповідей безпосередньо залежить від їх точності та спрямованості. Недостатньо чітко сформульовані промпти можуть призвести до отримання нерелевантної інформації або втрати важливих зв'язків. При використанні різних моделей LLM або при запитах у різний час відповіді можуть значно відрізнятися, особливо якщо відбуваються оновлення в даних або алгоритмах моделей, що може призвести до ускладнень у підтримці послідовності результатів, що знижує достовірність і передбачуваність отримуваної інформації.

Хоча рій автоматизує значну частину роботи, він також може підтримувати творчі та аналітичні процеси людини. Віртуальні експерти можуть генерувати ідеї, які надихають на нові підходи та рішення, а також надавати людині додаткову інформацію, на основі якої можна приймати більш обґрунтовані рішення.

Перспективи розвитку *«рою віртуальних експертів»* дуже широкі, особливо з урахуванням поточного розвитку LLM та можливостей їх використання в семантичному аналізі. Майбутнє цієї методології бачиться у створенні вдосконалених механізмів агрегування та фільтрації даних для підвищення узгодженості мережі та автоматичного вирішення суперечностей між відповідями віртуальних експертів, нових моделей взаємодії між людиною та LLM, де людина зможе більш гнучко керувати роями віртуальних експертів, задаючи точні критерії, що визначають, які відповіді слід вважати значущими та достовірними; покращенні механізмів узгодження ролей і контекстів, що дозволить досягати більш точного та комплексного аналізу без істотного втручання з боку людини.

РОЗДІЛ 12

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В OSINT: ІНСТРУМЕНТИ, МЕТОДИ ТА ЕТИЧНІ ВИКЛИКИ

Олексій БАРАНОВСЬКИЙ

Сучасний світ переживає безпрецедентний інформаційний вибух. До 2025 року обсяг даних, що генеруються у світі, за прогнозами, перевищить 181 зетабайт[1], що є колосальним стрибком у порівнянні з попередніми роками. Цей феномен, що отримав назву *«великі дані»* (**Big Data**), характеризується не лише величезним обсягом (**Volume**), але й надзвичайною швидкістю (**Velocity**) надходження нової інформації та її різноманітністю (**Variety**) — від структурованих баз даних до хаотичних потоків у соціальних мережах, відео, аудіо та зображень. Для дисципліни розвідки на основі відкритих джерел, яка за своєю суттю покладається на аналіз загальнодоступної інформації, ця нова реальність стала одночасно і даром, і прокляттям.

Традиційні методи OSINT, що базувалися на ручному та напівавтоматизованому пошуку, читанні та аналізі інформації аналітиками, виявилися неспроможними впоратися з цим *«інформаційним цунамі»*. Людські когнітивні та фізичні можливості мають свої межі; один аналітик або навіть ціла команда не в змозі обробити мільйони щоденних публікацій у соціальних мережах, тисячі годин відео, що завантажуються на платформи (Youtube, TikTok, Fasebook, X тощо), чи нескінченні потоки новинних стрічок. Це призводить до низки критичних

[1] Звіт компанії Statista. https://www.statista.com/statistics/871513/worldwide-data-created/

проблем, що підривають ефективність розвідки та розслідувань:

- **Інформаційне перевантаження та** *«шум»*: Величезна кількість нерелевантної інформації (*«шуму»*) ускладнює виявлення релевантних та цінних даних. Аналітики витрачають левову частку часу не на аналіз, а на фільтрацію та відсіювання непотрібного, що значно знижує ефективність та підвищує ризик пропустити критично важливі сигнали або докази.
- **Нездатність до оперативного реагування**: У сферах, де час є вирішальним фактором, традиційні методи аналізу стають практично неефективними. Загрози з'являються та поширюються за лічені хвилини, тоді як ручний аналіз може тривати годинами або й днями. Це перетворює OSINT з інструменту попередження на інструмент постфактум-аналізу.
- **Складність виявлення прихованих зв'язків**: Сучасні загрози, чи то скоординовані кампанії з дезінформації, чи то діяльність кіберзлочинних угруповань, часто мають складні, неочевидні патерни, розкидані по багатьох джерелах та платформах. Виявити такі зв'язки за допомогою ручного аналізу практично неможливо, оскільки вони стають видимими лише при обробці великих масивів даних.
- **Проблема верифікації та дезінформації**: Відкриті джерела за своєю природою вразливі до маніпуляцій, дезінформації та навмисного *«забруднення»* (intoxication). З появою технологій діпфейків та **генерації синтетичного контенту** відрізнити правду від вигадки стає дедалі складніше, що ставить під сумнів надійність усієї зібраної інформації.

Отже, традиційний OSINT, будучи переважно *реактивним інструментом*, зіткнувся з *кризою ефективності*, що вимагає переходу до нової, більш потужної та автоматизованої парадигми.

Відповіддю на виклики епохи великих даних стало впровадження технологій штучного інтелекту (*ШІ*) в практику OSINT. Ринок OSINT-рішень переживає експоненційне зростання, і за прогнозами, його обсяг збільшиться з приблизно $14.85 млрд у 2024 році до майже $38 млрд до 2030 року[2], причому ключовим драйвером цього зростання є саме інтеграція ШІ. Інтеграція штучного інтелекту не просто прискорює існуючі процеси, а фундаментально змінює саму філософію розвідки, забезпечуючи перехід від реактивного підходу до проактивного (*AI-Driven OSINT*).

Проактивна розвідка за допомогою ШІ, дозволяє не просто аналізувати минулі події, а й виявляти загрози на ранніх стадіях, прогнозувати їхній розвиток та запобігати їхній ескалації. Це досягається завдяки можливостям, які ШІ привносить у розвідувальний та розслідувальний цикли:

- **Автоматизація та масштабування збору даних**: ШІ-системи здатні в режимі 24/7 моніторити мільйони джерел — від соціальних мереж та блогів до форумів у Dark Web — і автоматично збирати релевантну інформацію, звільняючи аналітиків від рутинної роботи. Такі платформи, як Talkwalker[3], вже сьогодні сканують понад 150 мільйонів вебсайтів та десятки соціальних мереж, надаючи дані в реальному часі.
- **Глибинний аналіз неструктурованих даних**: Завдяки обробці природної мови (*Natural Language Processing, NLP*), ШІ може *«читати»* і розуміти величезні обсяги текстової інформації, виявляти ключові теми, аналізувати тональність висловлювань (*sentiment analysis*) та ідентифікувати зв'язки між сутностями, що було б неможливо для людини.
- **Розпізнавання образів та відеоаналіз (Computer Vision)**: Технології ШІ дозволяють автоматично аналізувати зображення та відео на предмет

[2] Звіт аналітичної компанії Mordor Intelligence. https://www.mordorintelligence.com/industry-reports/open-sourceintelligence- market
[3] https://www.talkwalker.com/

контексту та їх використання у новому розслідуванні може завдати невиправданої шкоди репутації людини, порушуючи її право на *«цифрове забуття»*.

- **Проблема інформованої згоди**: Хоча OSINT оперує публічними даними, користувачі, розміщуючи інформацію в соціальних мережах, часто не усвідомлюють, що їхні дані можуть стати об'єктом глибокого автоматизованого аналізу з боку державних чи комерційних структур. Це ставить під сумнів наявність реальної інформованої згоди на таку обробку.

Правові та регуляторні аспекти

Діяльність у сфері AI-driven OSINT відбувається у складному та часто невизначеному правовому полі, що створює значні ризики для операторів.

- **Дотримання законодавства про захист даних**: Нормативні акти, такі як Загальний регламент про захист даних (GDPR) в ЄС, накладають суворі обмеження на збір та обробку персональних даних, навіть якщо вони є публічними. Принципи мінімізації даних, обмеження мети та необхідності отримання згоди часто входять у прямий конфлікт з практикою масового збору даних в OSINT.
- **Транскордонні виклики та юрисдикція**: Інформаційний простір не має кордонів, і OSINT-розслідування часто охоплюють дані, що зберігаються в різних юрисдикціях з відмінним законодавством. Це створює правові колізії, пов'язані з законністю збору даних з іноземних серверів та їх подальшого використання як доказів.
- **Правова відповідальність та підзвітність**: Залишається відкритим питання, хто несе відповідальність у випадку, якщо рішення, прийняте на основі невірного висновку ШІ, завдасть шкоди особі чи організації. Непрозорість роботи багатьох моделей (*«чорна скринька»*) ускладнює процес аудиту та визначення причини помилки, що є перешкодою для побудови системи підзвітності.
- **Використання даних, отриманих незаконним шляхом**: OSINT часто перетинається з даними, які стали публічними внаслідок незаконних дій, наприклад, хакерських зламів та витоків. Використання таких даних у розслідуванні, навіть з благородною метою, створює складну правову та етичну дилему щодо *«плодів отруєного дерева»*.

МАЙБУТНЄ ШІ В OSINT: ІНТЕГРАЦІЯ ТА СИНЕРГІЯ

Перспективи розвитку AI-driven OSINT лежать у площині поглиблення синергії між людиною та машиною, а також інтеграції передових технологічних досягнень у сталі аналітичні практики. Майбутнє цієї дисципліни визначатиметься не стільки повною автономізацією розвідувальних процесів, скільки створенням ефективних гібридних систем, де обчислювальна потужність штучного інтелекту доповнює та посилює унікальні когнітивні здібності людини-аналітика. Це вимагатиме фундаментальних змін не лише в технологічному інструментарії, але й у методології, організаційних структурах та підготовці фахівців.

Центральною парадигмою майбутнього стає модель взаємодії *«Людина-ШІ»*, яка відкидає ідею повної заміни аналітика машиною. У цій концепції ШІ розглядається не як самостійний суб'єкт прийняття рішень, а виключно як досконалий інструмент, що виконує завдання, пов'язані з обробкою великих даних, виявленням патернів та автоматизацією рутинних операцій. Кінцева відповідальність за інтерпретацію отриманих результатів, застосування критичного мислення, професійного скептицизму та врахування складного соціокультурного контексту залишається прерогативою людини. Аналітик

майбутнього повинен еволюціонувати з ролі *«шукача інформації»* до ролі *«інтерпретатора знахідок ШІ»*, що вимагатиме формування нових компетенцій. Ключовими серед них стануть навички промпт-інжинірингу для ефективної взаємодії з мовними моделями, глибоке розуміння обмежень та потенційних упереджень ШІ-систем, а також високий рівень етичної та правової грамотності для відповідального використання цих потужних технологій[13].

У технологічному вимірі майбутній розвиток буде зосереджений на кількох ключових напрямках. Першочерговим завданням є розробка систем *«пояснюваного ШІ»* (Explainable AI, XAI), які здатні надавати прозорі та зрозумілі обґрунтування своїх висновків. Перехід від моделей типу *«чорна скринька»* до інтерпретованих систем є критично важливим для підвищення довіри до результатів ШІ та для їх ефективного використання у сферах з високою відповідальністю, таких як національна безпека та правосуддя. Одночасно відбуватиметься перехід до мультимодального аналізу, де ШІ-системи зможуть одночасно та комплексно аналізувати інформацію з різних джерел — тексту, зображень, аудіо та відео, — створюючи єдину, цілісну картину подій. Крім того, генеративний ШІ все активніше буде застосовуватися не лише для написання звітів, але й для симуляції складних сценаріїв та прогнозування розвитку кризових ситуацій, що дозволить моделювати потенційні відповіді на загрози у віртуальному середовищі.

На організаційному та стратегічному рівнях спостерігатиметься тенденція до все глибшої інтеграції OSINT з іншими, більш традиційними видами розвідки, такими як агентурна (HUMINT) та радіоелектронна (SIGINT). ШІ виступатиме як аналітичне ядро, що дозволить верифікувати та збагачувати дані із закритих джерел за допомогою публічної інформації, і навпаки. Це сприятиме формуванню єдиного розвідувального простору та підвищенню загальної ефективності. Одночасно, для відповіді на виклики, пов'язані з приватністю та безпекою, зростатиме попит на локальні та приватні ШІ-рішення, які дозволяють обробляти чутливу інформацію без її передачі на зовнішні сервери.

Правові та регуляторні рамки також зазнають еволюції; виникне необхідність у розробці гнучких, адаптивних норм, які б забезпечували належний контроль за використанням ШІ, захищали права громадян, але водночас не стримували технологічні інновації, що є життєво важливими для забезпечення національної безпеки. Етичні питання, що стосуються приватності, згоди та потенційного неправомірного використання технологій спостереження, вимагатимуть постійного діалогу між урядами, приватним сектором та громадянським суспільством для розробки стандартів відповідального використання ШІ.

РОЗДІЛ 13

LETSDATA ЯК ШІ-РАДАР ДЛЯ РАННЬОГО ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

Анатолій ВОЙТКО
Роман ОСАДЧУК

LetsData це ШІ-радар інформаційних операцій, що використовує ШІ для сканування мільйонів медійних повідомлень та публікацій у соціальних мережах, щоб ідентифікувати ранні сигнали інформаційних операцій, організованих кіберзлочинцями, ворожими країнами чи опонентами. Окрім

[13] Хмельков, А. В. (2024). Розвідка на основі відкритих джерел та штучний інтелект в практиці державного фінансового контролю. Соціальна економіка, 68, 212-226. https://doi.org/10.26565/2524-2547-2024-68-20.

іншого, LetsData фокусується на детекції:

1. *дезінформації, розкриваючи зманіпульовані відео та підробні документи, які мають на меті підривати довіру до організацій та урядів;*
2. *соціальної інженерії, щоб запобігти оманливим тактикам, спрямованим на обман співробітників, клієнтів та інвесторів у медіа та соціальних мережах;*
3. *синтетичних ідентичностей, які за допомогою неавтинтичної поведінки атакують інституції та організації;*
4. *астротурфінгу, для того щоб пересікати організовані кампанії, які формують фальшиву громадську думку, тощо.*

LetsData використовує набір технологій, які дозволяють отримувати швидкі сигнали з патернів публікацій та дозволяють вчасно й заздалегідь повідомляти користувачам про потенційні загрози, ключовими серед яких є Elasticsearch та Kibana.

ELASTICSEARCH

Elasticsearch – загальнодоступне програмне забезпечення, розподілена пошукова та аналітична база даних, яка забезпечує масштабований повнотекстовий пошук у режимі реального часу[1].

Elasticsearch з'явився 8 лютого 2010 р. як легковажний форк Apache Lucene, який написав із нуля ізраїльський розробник Шай Банон, прагнучи *«зробити пошук простим»* для свого домашнього кулінарного застосунку. Перший публічний реліз мав номер 0.4.0 і слоган *«You know, for search»*[2].

Архітектура Elasticsearch

- **Кластер** – це сукупність взаємопов'язаних вузлів (nodes), що спільно зберігають індекси й обслуговують запити.
- **Індекс** – логічний простір документів, що має:
  - *Mapping* – декларація полів та їх типи. Mapping може бути заданий або доповнений новими полями вручну або автоматично, на базі полів нового документу та автоматичного визначення їх типів. При цьому існуючи поля у mapping не можуть бути змінені.
  - *Alias* – псевдонім, який може вказувати на один або декілька індексів
- **Документ** – атомарна одиниця зберігання даних у форматі JSON

KIBANA

Kibana – це веб-інтерфейс та платформа візуалізації даних для Elasticsearch, яка дозволяє користувачам здійснювати пошук, аналізувати й візуалізувати великі об'єми даних у простому й зрозумілому вигляді. Kibana створив у 2013 р. інженер Рашид Хан як мінімалістичний веб-UI для візуалізації даних з Elasticsearch[3]. У 2015 р. Elastic, компанія, що стоїть за Elasticsearch, придбала Kibana та інтегрувала її в Elastic Stack (раніше відомий як ELK Stack), який включає Elasticsearch, Logstash і Kibana.

Kibana під'єднується до кластера Elasticsearch та надає чотири базові рівні роботи з даними:

- *ad-hoc дослідження (Discover)*
- *побудова візуалізацій (Lens/Visualize)*
- *композиція аналітичних панелей (Dashboards/Canvas)*
- *автоматизація (Alerting, ML-Jobs).*

[1] Elastic. Elasticsearch: The Official Distributed Search & Analytics Engine. https://www.elastic.co/elasticsearch.
[2] Elasticsearch Labs. Elasticsearch History: 15 Years of Indexing and Searching, February 12, 2025. https://www.elastic.co/search-labs/blog/elasticsearch-history-15-years.
[3] Kibana Explained. https://aijobs.net/insights/kibana-explained/.

Це робить Kibana центральним робочим місцем аналітика: від швидкого пошуку цитати до моніторингу хвилинних сплесків дезінформації.

Elastic Stack (Elasticsearch + Kibana + Logstash/Beats) став де-факто стандартом для збирання, індексування та інтерактивного аналізу великих обсягів неструктурованих текстових даних — від новинних стрічок і Telegram-каналів до повнотекстових архівів ЗМІ.

DISCOVER

Розділ Discover (*рис. 1*) у Kibana є основним інструментом для первинного аналізу даних, що зберігаються в Elasticsearch[4]. Він дозволяє дослідникам швидко переглядати, фільтрувати та досліджувати документи, надаючи можливість виявляти тренди, аномалії та інші важливі аспекти в текстових медіа-даних.

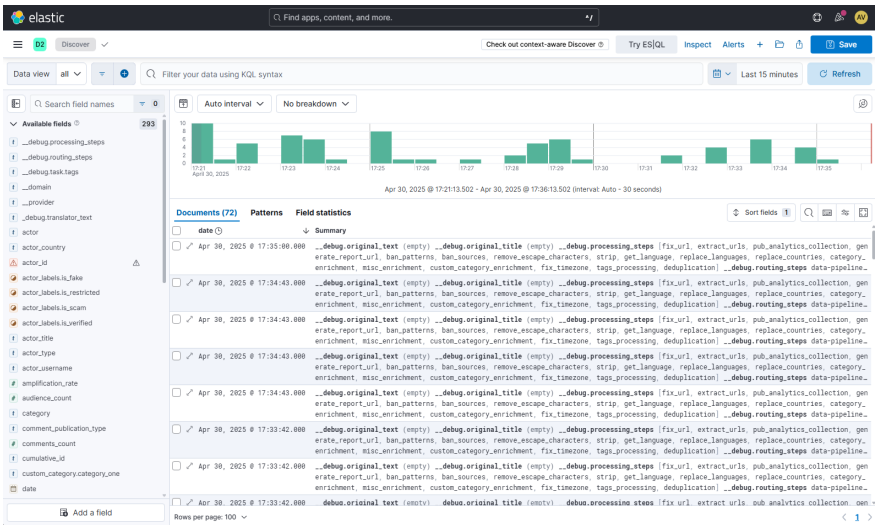

Рисунок 1. Інтерфейс Discover

Після відкриття Discover (*рис. 1*) користувач обирає відповідний Data View, який визначає, які індекси або потоки даних буде використовувати Kibana для відображення інформації (*рис. 2*). Якщо Data View ще не створено, його можна налаштувати, вказавши шаблон індексу (наприклад, news-*) та поле часу, яке буде використовуватися для фільтрації за часовими рамками.

У верхній частині інтерфейсу Discover знаходиться панель вибору часу, яка дозволяє встановити часовий діапазон для перегляду даних. Це може бути фіксований період (наприклад, останні 7 днів) або користувацький інтервал. Вибір часу впливає на всі відображені документи та візуалізації.

Основна частина Discover складається з таблиці документів та гістограми частоти подій. У таблиці відображаються документи, що відповідають вибраному Data View та часовому діапазону. Користувач може розгортати окремі документи для перегляду всіх полів та їх значень, а також застосовувати фільтри безпосередньо з інтерфейсу.

У лівій панелі Discover представлено список доступних полів. Користувач може шукати конкретні поля, переглядати їх найчастіші значення та додавати їх до таблиці документів для детальнішого аналізу. Це дозволяє швидко ідентифікувати ключові атрибути в даних.

Після налаштування фільтрів та перегляду даних користувач може зберегти поточний стан Discover як збережений пошук (Saved Search). Це дозволяє швидко повертатися до певного набору фільтрів та перегляду даних у майбутньому, а також використовувати збережені пошуки в інших частинах Kibana, таких як

[4] Explore Fields and Data with Discover | Elastic Docs. https://www.elastic.co/docs/explore-analyze/discover/discover-getstarted.

дашборди.

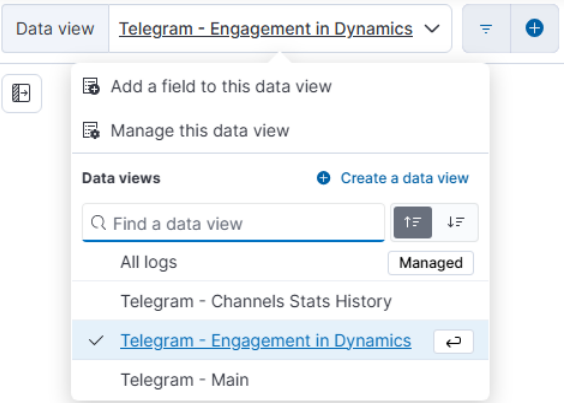

Рисунок 2. Приклад інтерфейсу вибору Data View

Для глибшого аналізу Discover надає можливість створювати візуалізації на основі вибраних полів. Наприклад, користувач може швидко побудувати графік розподілу значень певного поля або переглянути тренди у часі. Ці віз§уалізації можна зберігати та додавати до дашбордів для подальшого аналізу.

Discover дозволяє порівнювати кілька документів одночасно (*рис. 3*). Користувач може вибрати кілька записів у таблиці та переглянути їх поля поруч, що полегшує виявлення відмінностей та спільних рис між документами.

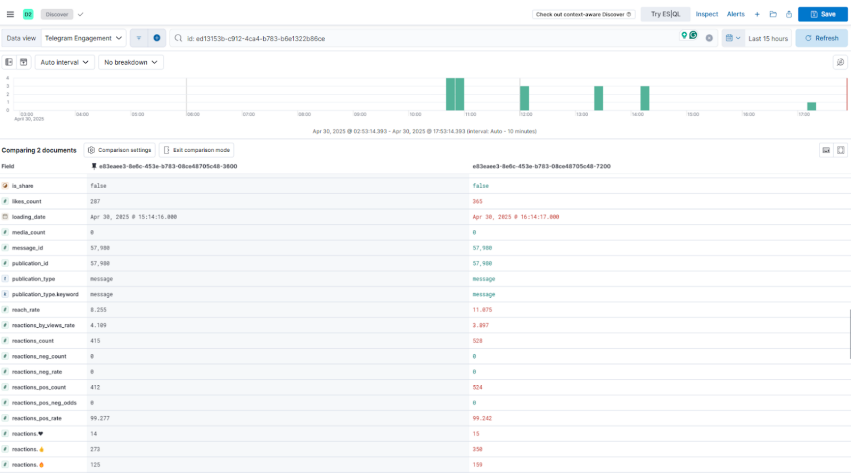

Рисунок 3. Приклад порівняння документів

Повнотекстовий та семантичний пошук у Kibana

Повнотекстовий пошук у Kibana забезпечується завдяки інтеграції з Elasticsearch і базується на використанні двох ключових пошукових мов:

- **KQL (Kibana Query Language)** – зручна і проста мова для швидкого пошуку за ключовими словами, яка дозволяє легко формулювати запити. KQL підтримує логічні оператори (AND, OR, NOT), пошук за фразами, діапазонами значень, а також інтуїтивну авто-підказку, що значно спрощує пошук текстових матеріалів. Приклад запиту:

  text: («вибори» or «парламент») and category.keyword: “Malign actor”

- **Lucene Query** – альтернатива для KQL, основною причиною використання якої є розширені функції Lucene, такі як регулярні вирази або нечітке

зіставлення термінів[5]. Однак синтаксис Lucene не може шукати вкладені об'єкти чи поля сценарію. Приклад запиту:

```
text: «вибори парламент»~5 AND category: "Malign actor"
```

- **ES|QL (Elasticsearch Query Language)** – розширена SQL-подібна мова, що дозволяє виконувати складні аналітичні запити з агрегацією і перетворенням текстових даних. Приклад запиту:

```
FROM *
| WHERE MATCH(text, 'вибори') AND date >= NOW() - INTERVAL 7 DAYS
| STATS count() BY date_histogram(date, '1 day')
| SORT date DESC
```

Під час виконання повнотекстового пошуку через інтерфейс Discover у Kibana, кожен документ у результатах має певне числове значення, позначене як _score. Це значення є показником релевантності документа до запиту, розрахованим Elasticsearch на основі обраної моделі ранжування (зазвичай це BM25).

_score не є просто відсотком або балом якості; це відносна метрика, яка залежить від частоти терміну в документі, довжини документа, частоти терміну в усій колекції документів, а також від типу запиту. Значення score дозволяє визначити, які документи найкраще відповідають змісту запиту, навіть якщо результати мають подібні ключові слова.

За замовчуванням Kibana не показує _score у списку полів у Discover. Щоб його побачити, користувач повинен додати поле _score вручну до таблиці результатів. Для цього потрібно:

- *ввести пошуковий запит у KQL (наприклад, body: «протест»)*;
- *у лівій панелі знайти поле _score (воно позначено як системне);*
- *натиснути на значок «додати до таблиці».*

Після цього стовпець _score з'явиться праворуч у таблиці документів, і можна буде порівнювати рівень релевантності різних результатів.

Високе значення score означає, що документ містить ключові слова, які точно збігаються з пошуковим запитом, і робить це в релевантному контексті (наприклад, у заголовку чи на початку тексту). Нижчі значення score свідчать або про часткові збіги, або про меншу важливість знайдених слів у структурі документа.

Наприклад, запит **title**: *«вибори»* може повернути десятки статей, але ті, в яких *«вибори»* згадано у назві, вступі й кілька разів у тілі тексту, отримають найвищий бал. Водночас документи, де згадка випадкова або в менш значущих розділах, матимуть нижчий _score.

Візуалізації

Kibana має набір інструментів для візуального аналізу даних, який дозволяє оперативно оцінювати тренди, динаміку та розподіл тематичних матеріалів.

Lens – це простий у використанні інструмент для створення візуалізацій[6]. Серед його особливостей – рекомендації щодо типу графіка на базі обраних даних, підтримка агрегацій та можливість швидкого переходу між різними типами графіків.

Dashboards – це інтерактивні панелі що складаються з різноманітних візуалізацій та дозволяють одночасно переглядати та аналізувати великі обсяги інформації

[5] Lucene Query Syntax | Elastic Docs. https://www.elastic.co/docs/explore-analyze/query-filter/languages/lucene-querysyntax.
[6] Lens | Elastic Docs. https://www.elastic.co/docs/explore-analyze/visualize/lens.

з різних джерел даних[7].

Canvas – це інструмент призначений для створення презентаційних матеріалів та інтерактивних інформаційних звітів на основі візуалізацій, що дозволяє налаштовувати шрифти, кольори та дизайн[8].

Lens

Kibana Lens – це інтуїтивно зрозумілий інструмент для створення візуалізацій у Kibana, який дозволяє користувачам легко перетворювати дані з Elasticsearch у графіки та діаграми за допомогою простого інтерфейсу перетягування[9]. Lens автоматично пропонує типи візуалізацій, які найкраще підходять для обраних даних, що спрощує процес аналізу та представлення інформації.

Щоб створити нову візуалізацію в Kibana Lens, потрібно перейти до розділу *Visualize* та натиснути *Create visualization*. У списку доступних типів візуалізацій потрібно обрати Lens. Відкриється робоча область, де можна почати створення візуалізації (*рис. 4*).

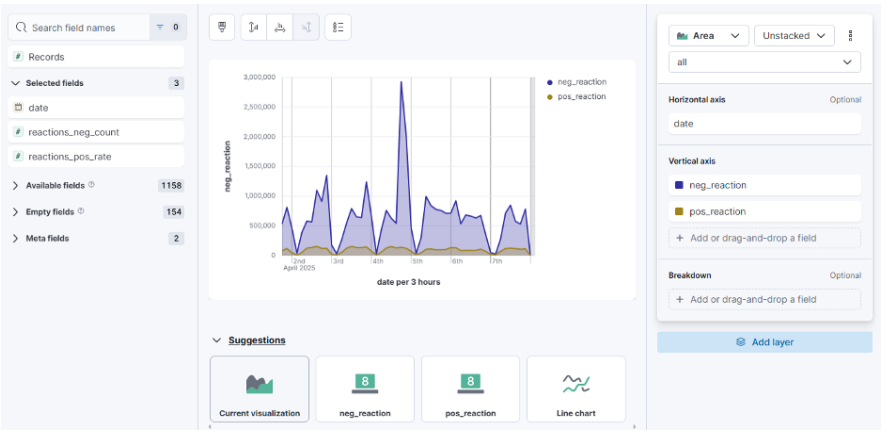

Рисунок 4. Приклад візуалізації в інтерфейсі Lens

У верхній частині інтерфейсу знаходиться випадаючий список для вибору Data View – це визначає, які індекси Elasticsearch будуть використовуватися для візуалізації. Потрібно обрати відповідний Data View, що відповідає даним.

У лівій панелі відображаються доступні поля з обраного Data View. Щоб додати поле до візуалізації, потрібно перетягнути його на робочу область. Lens автоматично визначить тип агрегації та запропонує відповідний тип графіка. Наприклад, перетягування числового поля може створити гістограму, а текстового – діаграму розподілу.

Після додавання полів можна налаштувати тип візуалізації, агрегації та інші параметри:

- **тип візуалізації**: у верхній частині робочої області можна змінити тип графіка (*наприклад, стовпчикова діаграма, лінійний графік, кругова діаграма тощо*);
- **агрегації**: натискаючи на поле в робочій області, можливим є змінити тип агрегації (*наприклад, середнє значення, сума, кількість унікальних значень*);
- **розбиття за категоріями**: додавання поля до секції *«Break down by»*, розбиває дані за певною категорією.

Серед типових візуалізацій в Lens для аналізу медіа-даних такі:

- *лінійні графіки (Line charts)* — аналіз трендів (згадки за день/годину, зміни

[7] Exploring Dashboards | Elastic Docs. https://www.elastic.co/docs/explore-analyze/dashboards/using.
[8] Canvas | Elastic Docs. https://www.elastic.co/docs/explore-analyze/visualize/canvas.
[9] Lens | Elastic Docs. https://www.elastic.co/docs/explore-analyze/visualize/lens.

тональності);

- *гістограми (Bar charts)* — порівняння кількості згадок по джерелах;
- *кругові діаграми (Pie charts)* — визначення частки медіа-контенту за тематикою або джерелом;
- *таблиці (Data tables)* — детальна інформація про топ-авторів, джерела або тематики;
- *treemaps і heatmaps* — візуалізація розподілу тем і активності джерел/

Lens підтримує багатошарові візуалізації, що дозволяє комбінувати різні типи графіків в одній візуалізації. Щоб додати новий шар, використовують кнопку Add layer та вибирають тип шару (наприклад, додатковий графік або лінія порівняння).

Для виконання математичних операцій над даними можна використовувати функцію Formula. Це дозволяє створювати нові метрики на основі існуючих полів. Наприклад, можна обчислити відсоткове співвідношення між двома полями або нормалізувати дані.

Lens дозволяє додавати анотації та референсні лінії до візуалізацій для підкреслення важливих подій або порогових значень. Це може бути корисно для вказівки на аномалії або ключові моменти в даних.

Можна застосовувати фільтри до всієї візуалізації або окремих шарів за допомогою Kibana Query Language (KQL). Це дозволяє зосередитися на певних підмножинах даних або порівнювати різні сегменти.

Після завершення налаштування візуалізації обирають *Save and return*, щоб зберегти її. Візуалізацію можна додати до існуючого дашборду або створити новий для подальшого аналізу та спільного використання.

Dashboards

Інтерфейс Dashboards у Kibana є ключовим інструментом для інтерактивного аналізу даних, що дозволяє користувачам візуалізувати, фільтрувати та досліджувати інформацію з Elasticsearch у реальному часі[10].

У верхній частині дашборду (*рис. 5*) розташована панель запитів, яка за замовчуванням використовує мову запитів Kibana Query Language (KQL). Це дозволяє формулювати точні запити для фільтрації даних. Під час введення запиту Kibana динамічно пропонує відповідні поля, оператори та значення, що полегшує процес формування запиту.

Фільтри, або *«filter pills»*, дозволяють зосередитися на конкретних даних. Їх можна додавати, взаємодіючи з візуалізаціями на дашборді або вручну через редактор фільтрів. Наприклад, клацнувши на певному сегменті діаграми, автоматично додається відповідний фільтр, який застосовується до всього дашборду.

Часовий діапазон, встановлений на дашборді, визначає, які дані відображаються. Можна встановити глобальний часовий діапазон для всього дашборду або налаштувати індивідуальний діапазон для окремих панелей. Це дозволяє аналізувати дані за конкретні періоди, що особливо корисно при вивченні тенденцій або аномалій у часі.

Автори дашбордів можуть додавати різноманітні елементи управління для полегшення фільтрації даних:

- *списки опцій (Options list):* дозволяють вибирати одне або кілька значень для фільтрації.;
- *повзунки діапазону (Range slider):* дають змогу встановити числові межі для фільтрації даних;

[10] Exploring Dashboards | Elastic Docs. https://www.elastic.co/docs/explore-analyze/dashboards/using.

- *повзунки часу (Time slider):* дозволяють вибирати часові інтервали для аналізу даних у динаміці.

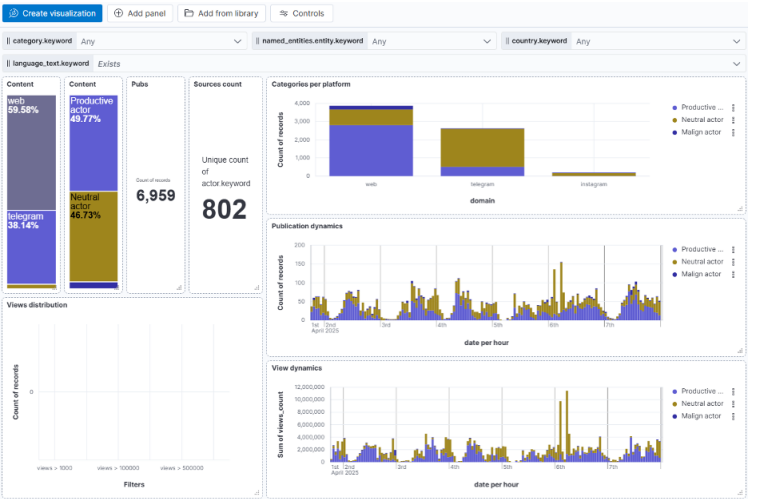

Рисунок 5. Приклад дашборду в інтерфейсі Dashboards

Для глибшого аналізу можна переглянути дані, що лежать в основі кожної панелі, а також запити, які використовуються для їх отримання. Це здійснюється через меню панелі, вибравши опцію *«Inspect»*. Користувач може переглянути дані у форматі таблиці, завантажити їх у форматі CSV, а також ознайомитися з запитами, що надсилаються до Elasticsearch.

Для зосередження уваги на певних візуалізаціях Kibana пропонує повноекранний режим дашборду, а також можливість максимізації окремих панелей. Це особливо корисно під час презентацій або детального аналізу конкретних аспектів даних.

Функціонал дашбордів у Kibana надає потужні інструменти для інтерактивного аналізу даних. Завдяки гнучким можливостям фільтрації, налаштування часових рамок та інтерактивним елементам управління, дослідники можуть ефективно вивчати текстові медіа-дані, виявляти тенденції та приймати обґрунтовані рішення на основі отриманих інсайтів.

Canvas

Kibana Canvas – це інструмент візуалізації та презентації даних, який дозволяє створювати динамічні, багатосторінкові, піксельно точні дисплеї, поєднуючи живі дані з Elasticsearch з кольорами, зображеннями, текстом та іншими елементами дизайну[11]. Canvas ідеально підходить для користувачів, які мають як технічні навички, так і творчий підхід до представлення даних.

Робоче полотно (workpad) – це простір, де створюються презентації живих даних (*рис. 6*). Можливим є створювати полотно з нуля, використовувати попередньо налаштоване полотно, імпортувати існуюче або скористатися зразком даних.

Кроки для створення нового полотна:

- *на сторінці Canvas натисніть Create workpad;*
- *вкажіть налаштування полотна;*
- *додайте назву;*
- *встановіть ширину та висоту або виберіть один із стандартних макетів;*
- *виберіть колір фону.*

[11] Canvas | Elastic Docs. https://www.elastic.co/docs/explore-analyze/visualize/canvas

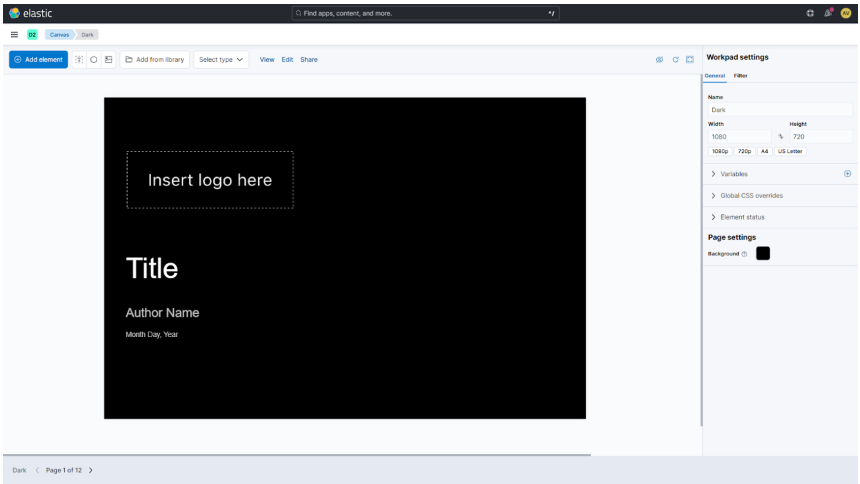

Рисунок 6. Шаблон презентації в інтерфейсі Canvas

Canvas пропонує різноманітні елементи для візуалізації даних:

- *графіки:* областеві, бульбашкові, координатні, пончикові, стовпчикові тощо;
- *текстові блоки:* форматуються за допомогою Markdown;
- *зображення:* можуть повторюватися або змінюватися залежно від даних;
- *форми:* для створення візуальних елементів дизайну;
- *фільтри:* випадаючі списки, повзунки діапазону та часу для інтерактивної фільтрації даних.

Щоб додати елемент: *обрати Add element – обрати потрібний тип елемента – розмістити його на полотні та налаштувати відповідно до потреб*.

Canvas дозволяє експортувати робочі полотна у форматі PDF або PNG для подальшого використання або спільного доступу.

Кроки для експорту: *обрати Share – обрати формат експорту (PDF або PNG) – налаштувати параметри експорту та натиснути Generate*.

Kibana Canvas є потужним інструментом для створення динамічних, інтерактивних презентацій на основі даних Elasticsearch. Завдяки широким можливостям налаштування та інтерактивності, Canvas дозволяє ефективно представляти дані в привабливому та зрозумілому вигляді.

Anomaly Detection (Виявлення аномалій)

Інструменти машинного навчання (Machine Learning, ML) у Kibana забезпечують автоматичне виявлення аномалій у даних, що є важливим для оперативного виявлення інформаційних криз, сплесків дезінформації або незвичних медіа-активностей[12].

Сценарії застосування:

- **виявлення незвичних піків активності** – модель виявляє несподіване зростання кількості згадок певної тематики, наприклад, сплеск кількості публікацій з певними згадками чи повідомлень у соціальних мережах;
- **аналіз зміни числових метрик** – модель знаходить аномальні відхилення метрик (перегляди, поширення, тощо), що можуть вказувати на нетипову медіа-активність, використовуючи історичні дані для навчання.

[12] “Anomaly Detection | Elastic Docs.” https://www.elastic.co/docs/explore-analyze/machine-learning/anomaly-detection.

Для створення завдання виявлення аномалій необхідно:

- у розділі Machine Learning перейти на вкладку Anomaly Detection;
- натиснути Create job, та обрати Single metric job, Multi-metric job, або Population job;
- обрати відповідний Data View;
- обрати поле (або поля) для аналізу;
- налаштувати параметри завдання, такі як:
  - *Bucket span*: інтервал часу для агрегації даних (наприклад, 1 год)
  - *Detector function*: функція для виявлення аномалій (наприклад, mean, sum, count)
  - *Influencers*: поля, які можуть впливати на результати аналізу.

Далі відкривається попередній перегляд параметрів завдання. Кнопка Create job запускає задане завдання.

Після запуску завдання можна переглянути результати:

- *Anomaly Explorer:* надає огляд усіх виявлених аномалій з можливістю фільтрації за різними параметрами.;
- *Single Metric Viewer:* дозволяє детально переглянути часовий ряд для окремої метрики та виявлені аномалії.

У цих інтерфейсах можна додавати анотації, переглядати впливові фактори та аналізувати деталі кожної аномалії (*рис. 7*).

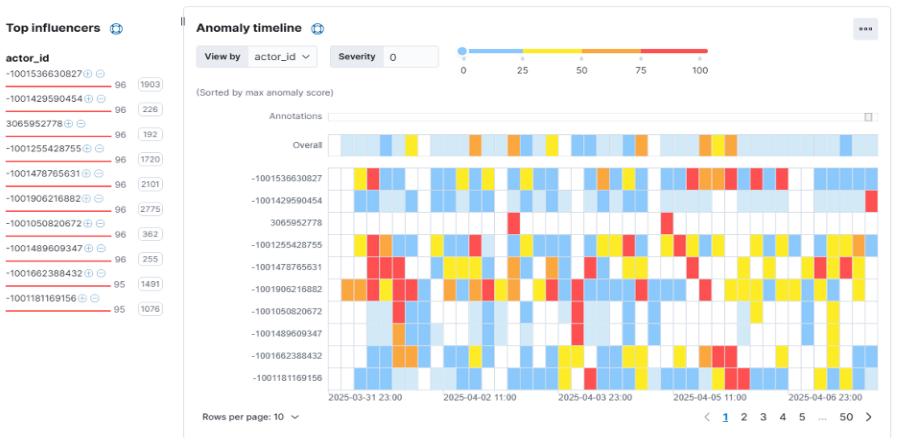

Рисунок 7. Приклад результату виявлення аномалій у переглядах для окремих Telegram каналів

Також Kibana дозволяє створювати прогнози на основі наявних даних:

- у *Single Metric Viewer* обрати завдання, для якого потрібно створити прогноз;
- обрати *Forecast*, вказати тривалість прогнозу та обрати *Create*.

Прогнозовані значення відображатимуться разом з фактичними даними, що дозволяє оцінити майбутню поведінку системи.

Всі ці інструменти, а також набір внутрішніх алгоритмів LetsData використовується для раннього виявлення загроз в інформаційному просторі. *Раннє виявлення* – одна з головних задач інструментів та команди, оскільки завданням інструменту є інформування клієнтів про інформаційні операції у момент їхньої появи в інформаційному просторі. Аналітики та дослідники можуть використовувати наявні візуалізації для швидкого аналізу інформаційного простору, пошуку аномалій та точок інтересу, тобто сигналів,

які треба дослідити детальніше. Візуальний пошук спрощує роботу та дозволяє побачити артефакти набагато швидше, зменшуючи час між виявленням та повідомленням про загрозу, а тому й реакцією на такі інформаційні загрози та операції.

Повідомлення про загрозу, до того як ця інформація отримає поширення у багатьох джерелах, надає клієнтам з державного та недержавного сектору бути готовими до відбиття інформаційних загроз. Чим швидше клієнти отримують сигнал про інформаційну операцію – тим більша вірогідність того, що така операція не буде успішною, що доведено серед іншого державними органами, бізнесом та громадянським суспільством України під час широкомасштабного вторгнення РФ в Україну у лютому 2022 року. Саме швидке розбиття російською дезінформації дозволило мінімізувати вплив російських інформаційних кампаній в Україні на початку вторгнення й надалі. Щоб продемонструвати практичне використання зазначеного технологічного рішення, нижче наведений приклад, де продуктовий та технологічний сет інструментів дозволив побачити інформаційну кампанію у її зародку та прозвітувати протягом кількох годин з моменту її появи й до того, як історія набула масового поширення.

Приклад використання технологій Elasticsearch та внутрішнього набору інструментів

Elasticsearch використовується для відслідковування аномалій та змін в інформаційному просторі й дозволяє бачити первинні сигнали інформаційних операцій у цифровому просторі. За допомогою візуальної репрезентації, аналітики можуть отримати перший сигнал щодо певної теми, активності специфічних акторів, та патернів координованої неавтентичної поведінки, тобто сигналів про те, що хтось навмисне маніпулює інформацією та видає себе за когось іншого чи штучно збільшує популярність певного контенту. За допомогою цього інструменту та набору пропрієтарних технологій, LetsData надає послуги з раннього інформування про загрози й дозволяє урядовим та неурядовим організаціям бути попереду в інформаційному просторі та знати про інформаційні операції заздалегідь, щоб мати можливість підготувати вчасну відповідь.

Один з успішних прикладів роботи організації стався у жовтні 2024, коли міжнародна організація, яка спеціалізується на протидії інформаційним операціям та підвищенню інформаційної стійкості у країнах Європи співпрацювала з LetsData, щоб моніторити та аналізувати інформаційні загрози та операції у країнах східної Європи[13].

У жовтні 2024 року LetsData, AI радар проти інформаційних загроз, помітила нову загрозу у вигляді публікації про депортаційні табори у одній з країн східної Європи. Інформаційна операція продовжувалась кілька діб, а факт-чекінг та заперечення від офіційних осіб були опубліковані занадто пізно, що дозволило операції бути доволі успішною та широко розповсюджуватись кілька днів.

Вранці першого дня операції, кілька шкідливих акторів у Телеграмі опублікували інформацію, яка навмисно спотворила публікацію довіреного закордонного медіа, щоб надати достовірності наративу, який експлуатував страхи перед міграцією та підсилював недовіру до інституцій місцевого уряду та Європейського Союзу загалом.

Внутрішня система сповіщення загроз LetsData дозволила знайти аномалію в інформаційному просторі в момент перших кількох публікацій, до того як кампанія набула широко розповсюдження. Первинне сповіщення міжнародної організації, яка співпрацює з LetsData, у вигляді короткого звіту, що зафіксував наявність таких повідомлень, відбулось впродовж 4 годин з моменту

[13] Kalenský, Jakub, and Roman Osadchuk. “How Ukraine Fights Russian Disinformation: Beehive vs Mammoth.” Hybrid CoE Research Report 11. Hybrid CoE, January 24. https://www.hybridcoe.fi/wp-content/uploads/2024/01/20240124-Hybrid-CoE-Research-Report-11-How-UKR-fights-RUS-disinfo-WEB.pdf.

першої публікації, коли лише кілька згадок про цей інцидент та статтю було задокументовано, що демонструє швидкість та деталізацію алгоритмів та підходів команди LetsData. На графіку (*рис. 8*) можна побачити кількість публікацій у конкретний проміжок часу. Під час появи перших публікацій вранці 6 жовтня, вже опівдні короткий звіт було надіслано міжнародній організації з повідомленням про те, що такий наратив вже шириться мережею.

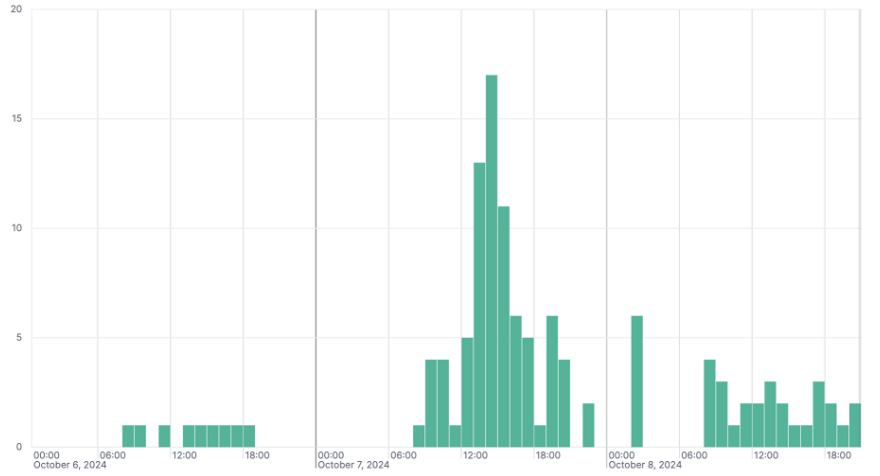

Рисунок 8. Графік кількості публікацій на тему "депортаційних таборів" по часу

Впродовж першого дня операції цю історію опублікували лише 9 джерел, які відслідковувала команда та алгоритми LetsData. Наступного дня, LetsData сповістила про новий сплеск уваги до наративу з боку великої кількості акторів, які відкрили для себе та почали просувати історію. Команда надіслала другий інформаційний звіт, вказуючи, що історія набуває великих масштабів та потребує негайного спростування та реагування на цю загрозу. Цей звіт LetsData надійшов до міжнародної організації у момент до того, як історія отримала надзвичайний сплеск уваги й була поширена більш ніж десятки разів у різних джерелах – від медіа до Телеграм каналів, та до першого офіційного факт-чекінгу від журналістів. Загалом історія набула широкого розголосу та масштабу з більш ніж 120 публікаціями про цю публікацію, що дозволило досягти досить великої аудиторії та посіяти недовіру до демократичних інституцій.

Така затримка у реакції призводить до того, що деякі інформаційні операції залишаються без уваги досить довгий час, дозволяючи встановити порядок денний та заповнити інформаційну пустку до офіційної чи перевіреної інформації. Це створює сприятливі умови для маніпуляцій, коли аудиторія починає орієнтуватися не на факти, а на емоційні й часто неправдиві повідомлення.

Ця проблема є повсюдною та не є унікальною для конкретної країни, організації чи структури. Вона демонструє слабкість традиційних інструментів та інституцій у детекції, пошуку та розумінні сучасних інформаційних операцій, які відбуваються у більших масштабах через розвиток технологій, платформ розповсюдження інформації та, насамперед, штучного інтелекту. Сучасні інформаційні операції стають дедалі більш складними, адаптивними та здатними маскуватися під легітимні інформаційні потоки, що значно ускладнює їх виявлення на ранніх етапах.

Інформаційні операції (InfoOps), такі як неправдиві заяви про існування депортаційних таборів ЄС у Молдові, призначені для використання суспільних страхів, загострення соціального напруження та підриву довіри до інституцій. Якщо їх не зупинити, такі наративи можуть поширюватися лавиноподібно,

впливаючи на громадську думку, мобілізуючи протестні настрої, стимулюючи антизахідні або антидержавні настрої та поглиблюючи політичну й соціальну поляризацію. У довгостроковій перспективі це може призводити до дестабілізації демократичних процесів, делегітимізації державних органів та ослаблення міжнародних партнерств.

Цей випадок демонструє, наскільки важливим є раннє виявлення для протидії цим загрозам. Виявлення та аналіз наративу за 24 години до його піку, яке здійснила LetsData, забезпечило неоціненний час на розробку контрнаративу, інформаційного втручання та перевірку фактів. Це не просто дозволило мінімізувати шкоду – це продемонструвало потенціал руйнування шкідливої кампанії ще до її ескалації, уникнувши більш широкого резонансу.

Цей приклад підкреслює необхідність моніторингу в реальному часі та проактивних стратегій для ефективної протидії інформаційним операціям. Суб'єкти, які мають змогу виявляти та реагувати на нові наративи на ранній стадії, краще підготовлені щодо захисту громадської думки, підтримки інституційної довіри та пом'якшення впливу скоординованих інформаційних загроз.

У світі, де зловмисні актори дедалі частіше використовують легітимні інформаційні канали – включно із соціальними мережами, мейнстрім-медіа та навіть офіційними заявами – для поширення дезінформації, випереджальне реагування більше не є конкурентною перевагою. Це критично необхідна умова, яка визначає здатність суспільства протистояти маніпуляціям, зберегти інформаційну безпеку та забезпечити стійкість до гібридних загроз.

РОЗДІЛ 14

ІНФОРМАЦІЙНО-АНАЛІТИЧНІ ЗАСОБИ МОНІТОРИНГУ ТА ПРОГНОЗУВАННЯ У СИСТЕМІ СИТУАЦІЙНОЇ ОБІЗНАНОСТІ

Елліна ШНУРКО-ТАБАКОВА

Ситуаційна обізнаність як термін військової теорії (авіації) отримав оновлення та популяризацію в умовах гібридної агресії рф проти України у середовищі фахівців та експертів з стратегічних комунікацій. Зазвичай Ситуаційну обізнаність (СО) згадують як необхідний чинник для прийняття рішень (ПР). Оскільки стратегічні комунікації притаманні всім аспектам життєдіяльності держави та народу, стосуються фактів та процесів всього інформаційного простору, то стандартів визначень та вимог до фіксації фактів і процесів, їх розуміння та відображення у прогнозуванні, - майже відсутні. У результаті сфера комунікацій оперує фактами з отриманих багаточисельних систем моніторингу і одразу намагається приймати оперативні та стратегічні рішення. Аналіз та розуміння СО віддані персоналіям, що займають посади, які також не містять галузевих стандартів, зокрема – навичок в обробці та інтерпретації даних.

За умови гібридних атак та впливів окрім комплексного синтезу інформації (обробки сигналів та траєкторій у *«простих випадках»* кінетичних атак), необхідні урахування виявлених сенсів та досягнення розуміння цілей та сценаріїв інформаційних кампаній. Фактично, будь-яку гібридну загрозу можна розкласти на класичну та її цифрову складову. Кожну складову можна описати відповідними статистичними рядами.

Кожна складова цифрової безпеки має правила/досвід/засоби розбудови систем збирання та збереження даних й рішення, що відстежують існуючі проблеми,

оцінюють ризики інцидентів, правила захисту та протидії загрозам. Сучасні технічні засоби працюють не лише з відомими загрозами (наприклад, вірусами), але й за допомогою технологій штучного інтелекту прогнозують та виявляють нові загрозливі втручання в інформаційні системи.

Щодо публічної або медійної складової – засоби відстеження та ідентифікації інформаційних загроз або маніпулювання не можуть мати однозначних відповідей у багатьох випадках та вимагають вміння працювати з великими обсягами інформації (Big Data). А це передбачає використання аналітичного й математичного інструментарію фахівцями із забезпечення безпеки, зокрема у розрізі оцінювання та реагування на інформаційні загрози.

Першим кроком в оцінюванні загроз має бути ситуаційна обізнаність щодо контексту ситуації, конкретних наборів даних відносно предмета загрози, теми, особистості або процесів.

Формування ситуаційної обізнаності має починатися з аналізу статистичних даних за обраними тематичними групами, наприклад:

- економічні та фінансові показники;
- підприємницька діяльність/зв'язки;
- дані міністерств та відомств (статистичні, реєстри тощо);
- активність громадського сектора;
- мобільний-трафік;
- інтернет-трафік;
- трансакційний трафік;
- захворювання;
- надзвичайні події;
- злочини та правопорушення;
- кіберподії – заподіяні та попереджені.

Наступний крок – моніторинг/відстеження показників або специфічних характеристик за такими групами:

- аналітичні показники статистичних даних;
- спеціалізовані системи;
- персональні системи відстеження;
- системи оповіщення (гугл трендс, спеціалізовані);
- соціальні мережі – особи, відкриті та таємні групи;
- інтернет-контент – загальний, спеціалізований, державний, таємний;
- канали комунікаційних платформ.

Оптимальна кількість необхідних статистичних рядів для спостереження має формуватися за принципом достатності фіксації характеристик, що свідчать про спокійний та кризовий стани *Об'єкта* відстеження. Досить часто задля СО щодо багатопланового *Об'єкта* необхідна декомпозиція за темами, напрямками, персоналіями тощо.

Приклад: створення системи ситуаційної обізнаності для загроз кібердії

Необхідне онлайн спостереження, наявність ретро даних, зберігання первинних даних (мінімум - щотижнева основа):

- перехоплення конфіденційної інформації,
- знищення інформації,

- підміна інформації,
- зупинка інформаційних сервісів,
- зупинка підприємств,
- порушення функціонування державних сервісів,
- порушення функціонування об'єктів критичної інфраструктури,
- створення заражених мереж,
- розповсюдження вірусів, DDoS атаки,
- приховані збирання, використання або продаж даних,
- психологічний вплив з кібернаслідками (шантаж)

Статистика:

- класифікація та реєстрація кібератак за технологіями, походженням, об'єктом впливу, ступенем загрози;
- міжнародні дані щодо нових технологій кібероперацій;
- міжнародний досвіду протидії;
- дані щодо можливостей попередження конвертації технологій у кримінальну сферу.

Моніторинг:

- узагальнення власного досвіду розслідувань;
- виявлення технологічних можливостей проникнення до систем та ресурсів;
- виявлення спаму, вірусів;
- відстеження налаштувань внутрішніх користувачів;
- відстеження та захист від DDoS атак;
- відстеження психологічного впливу;
- відстеження Darknet та таємних груп;
- виявлення скомпрометованих персоналій;
- відстеження ключових запитів, тем та персоналій

Для роботи у спеціалізованих системах моніторингу важлива коректна *Декомпозиція* гібридних викликів до тем. Розуміння контексту суспільно значущої інформації має важливе значення у питаннях декомпозиції загроз в інформаційному середовищі до тем та їхнього семантичного ядра, що є основою ключових запитів у системах моніторингу (*рис. 1*). Зрозуміло, що дискредитація певного чиновника державного органу здійснюється не назвою статті *«Сьогодні дискредитуємо чиновник N ...»*, а підбором негативних та емоційних тем навколо діяльності обраного об'єкта атаки.

Інформаційне супроводження загроз кібердії з боку РФ може бути декомпозовано до таких складових:

- відсутність кваліфікованих кадрів в Україні;
- переваги у підготовці кібервійськ рф;
- протиставлення державного, громадського та бізнесового секторів за професійними якостями;
- апокаліптичні сценарії;
- дискредитація сегменту впливу (керівництва, галузі тощо);

- чутки та фейки за темами;
- тригери зростання з початком операцій;
- перебільшення результатів ще до початку;
- попередження систем оповіщення;
- активність у таємних групах, Darknet, спеціальних групах.

Тематичне супроводження/редакційне завдання загроз кібердії:

- недоліки системи навчання кібервійськ;
- історії успіхів хакерів рф;
- дискредитація якості та стійкості кадрів;
- від хайпів до розслідувань;
- висвітлення дій хакерів;
- дискредитаційні матеріали щодо теми;
- чутки та фейки за темою;
- тригери зростання з початком операцій за темою;
- персоналізоване спостереження.

Рисунок 1. Семантичне ядро опису кібернетичних загроз в інформаційному просторі

Саме ключові слова, що відображають певну тему для відстеження – моніторингу є предметом особливої уваги – їх кількість повинна бути вичерпною, обмеженою, не занадто широкою на етапах дослідження визначених обставин. Завжди потрібно йти від широкого до вузького кола дослідження і бути у контексті подій, щоб вчасно зупинитися і не втратити важливий вислів, ім'я спікера, часові параметри[1].

Автоматизований сервіс моніторингу, аналізу та прогнозування Атак Індекс працює з актуальними та архівними базами даних моніторингу веб джерел та соціальних мереж.

За ключовими словами Користувач отримує стандартний звіт, що містить 37 діаграм та 60 аналітичних параметрів (*рис. 2*). Компактний або звернутий звіт містить 12 розділів, що організовані за принципом пазлів, що розгортаються за потребою. Можна також в один клік отримати одразу повністю розгорнутий

[1] Стратегічні комунікації в умовах гібридної війни : погляд від волонтера до науковця : монографія / [Слухай Н. В., Яворська Г. М., ... Романюк В. С. та ін. ; за заг. ред. Компанцевої Л.] ; Нац. акад. Служби безпеки України. - Київ : [Національна академія СБУ], 2021.;

звіт. Пошук здійснюється по всіх обраним базам даних за заданим часовим інтервалом. Сервіс не вимагає додаткового програмування або підготовки тематичних вибірок. Бази даних містять ретроспективні результати моніторингу глибиною понад 20 років кириличного та англійського сегменту світового інформаційного простору з понад 60 країн.

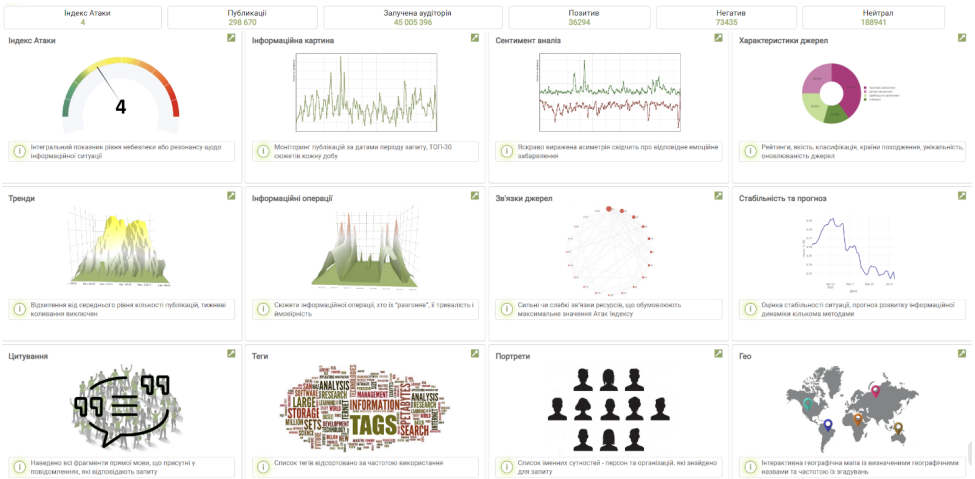

Рисунок 2. Приклад вмісту аналітичного змісту

Автоматизований сервіс моніторингу, аналізу та прогнозування Атак Індекс створено командою, що має надзвичайний науковий та організаційний досвід, включно з протидією пропаганді з 2014 року. Остання версія вітчизняного стартапу працює з 2024 року є органічним поєднанням наукових розробок, авторських творів і їх втіленням у бізнес-моделі на інноваційних ринках.

Атак Індекс є формулою, що захищено авторським свідоцтвом і включає аналітичні показники, які є невід'ємною частиною сервісу і детально описані у відповідних частинах автоматизованого звіту. Розрахунки за єдиною формулою для кожного запиту забезпечує коректне співвідношення величин індексу на однаковому інтервалі часу. У роботі порівнюються показники різних тем у відповідних часових інтервалах.

Атак Індекс – запатентована формула, що містить параметри звіту та розраховується для кожного запиту до сервісу з огляду на значення характеристик, що можуть свідчити про небезпечні явища в інформаційній ситуації (різке зростання негативу або наявність інформаційний ситуацій).

Повнота сервісу є однаковою для будь-якого користувача, залежно від умов доступу – з повними правами доступу до всього обсягу даних – ретроспективою більш 20 років.

Оновлення кожних 15 хвилин охоплює близько 20 000 веб-сайтів, в 64 країнах світу, для сегментів кирилиці та латиниці. Система отримує більше 120 000 документів на добу. Накопичений обсяг публікацій в інформаційному сховищі перевищує 700 мільйонів публікацій та щомісяця збільшується на більше ніж 3 млн публікацій (*рис.3*). Також зняття та запис інформації здійснюється з соціальних мереж за обраними запитами або каналами, щоденне поповнення складає близько 100 000 публікацій.

Запити до всіх баз даних здійснюються за допомогою ключових слів.

Моніторинг здійснюється по таким соціальним мережам: Facebook, LiveJournal, LiveInternet, Vkontakte, Odnoklassniki, Telegram, Twitter, YouTube, Reddit, Weibo, RuTube, Medium, ArXiv, Academia.

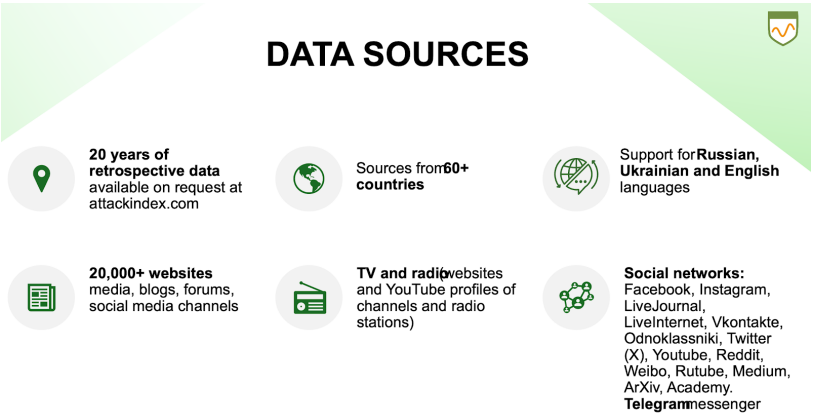

Рисунок 3. Інформаційні ресурси Атак Індекс

Типова текстова інтерпретація кожного з 10 балів Атак Індекс:

0 – *«За вашим запитом інформація відсутня. Можливо, про вас ніхто не знає або ключові слова обрані неправильно.»*

1 – *«Інформація практично не поширюється, носить епізодичний і ситуативний характер. Можливо, ключові слова спливають у зв'язку з незалежними від вас подіями.»*

2 – *«Ситуація пасивна, мало суб'єктів, зацікавлених у її поширенні. Вашому об'єкту нічого не загрожує. Інформаційний фон є органічним та не має штучних сплесків.»*

3 – *«Низька активність має природний характер. Спостерігається органічна реакція у зв'язку зі зв'язаними заходами. Можлива підготовка до інформаційної атаки, аналізуйте часові рамки і співвідношення негативу та позитиву.»*

4 – *«Досить насичене інформаційне поле свідчить про актуальність теми або участь у резонансних подіях. Органічний характер поширення інформації свідчить, що інформація представляє інтерес. Залежно від залучення джерел можна судити про величину відгуків аудиторії та значущість проведених заходів.»*

5 – *«Активність мережевих джерел вимагає вашої уваги і реакції у вигляді власних інформаційних заходів. Насичене інформаційне поле свідчить про актуальність теми або участь у резонансних подіях. Органічний характер поширення інформації свідчить, що інформація представляє інтерес. Залежно від залучення джерел можна судити про величину відгуків аудиторії та значущість проведених заходів.»*

6 – *«Рівень небезпеки для досліджуваного об'єкта досить відчутний. Уважно вивчіть джерела, динаміку і дати появи провокаційних матеріалів. Найімовірніше, вони співвідносяться з діяльністю особи або організації, вказаної вами в ключових словах. У розділі |»Учасники|» ви знайдете ініціаторів та імена людей/назви ресурсів, які підтримали інформаційну атаку. Часто ініціаторами стають маловідомі сайти або профілі в соціальних мережах. Буває так, що опубліковану ними інформацію цитують авторитетні ЗМІ.»*

7 – *«Є всі ознаки присутності штучного впливу і наявності інформаційної операції. Відхилення від середнього рівня інформаційного потоку свідчать про інтенсивну інформаційну атаку. Уважно вивчіть джерела, динаміку і дати появи провокаційних матеріалів. Найімовірніше, вони співвідносяться з діяльністю особи або організації, вказаної вами в ключових словах. У розділі |»Учасники|» ви знайдете ініціаторів та імена людей/назви ресурсів, що беруть участь у поширенні інформації. Часто ініціаторами стають маловідомі сайти або*

профілі в соцмережах. Буває так, що опубліковану ними інформацію цитують авторитетні ЗМІ.»

8 – *«Виявлено типові ознаки наявності інформаційної операції. Вказана вами компанія/персона може виявитися головним об'єктом її розробки. Активна фаза відповідає датам ..... . Якщо розглядається поточний час, слід негайно відреагувати на інформацію, опубліковану в перерахованих нижче джерелах. З'ясуйте, хто був ініціатором, і підготуйте інформаційні контрзаходи. Якщо ви керівник компанії, зверніться до менеджера зі зв'язків із громадськістю та співробітника, який відповідає за антикризовий PR. У разі ретро-дослідження слід проаналізувати джерела-ініціатори, інформаційні повідомлення та їх однорідність, хто був зацікавлений у поширенні інформації.»*

9 – *«Аналіз досліджуваного запиту демонструє типове поєднання розгорнутої інформаційної операції, інтенсивного поширення основного удару і підтримки процесу зацікавленими особами. Можливо вами, якщо це контрольоване захід. :) Процес стабільний і буде таким самим, як і на досліджуваному періоді. Зазначена вами компанія/персона стала головним об'єктом її розробки. Активна фаза відповідає датам %PERIOD%. Можливо, ви частина події або явища і не можете бути відокремлені в інформаційно незалежні потоки. Якщо розглядається поточний час, слід негайно відреагувати на інформацію, опубліковану в перелічених нижче джерелах. З'ясуйте, хто був ініціатором, і підготуйте інформаційні контрзаходи. Якщо ви керівник компанії, зверніться до менеджера зі зв'язків з громадськістю та співробітника, який відповідає за антикризовий PR. У разі ретро-дослідження слід проаналізувати джерела ініціатори, інформаційні повідомлення та їх однорідність, хто був зацікавлений у поширенні інформації. Пам'ятайте, що лише активна участь, створення альтернатив і привернення уваги може призвести до контролю ситуації і подолання негативних наслідків.»*

10 – *«Ви в епіцентрі суспільно значущої події. Більш того - процес нестабільний і може розвиватися непередбачуваним чином. Можуть залучатися інші події і змінювати характер і інтенсивність поширення інформаційних хвиль. Пам'ятайте, що лише активна участь, створення альтернатив і привернення уваги можуть привести до контролю ситуації та подолання негативних наслідків. Аналіз досліджуваного запиту демонструє типове поєднання розгорнутої, яскраво вираженої інформаційної операції, інтенсивного поширення основного удару та підтримки процесу зацікавленими особами. Можливо, вами, якщо це контрольований захід. Зазначена вами компанія/персона стала головним об'єктом її розробки. Активна фаза відповідає датам операції: ..... . Можливо, ви частина події або явища і не можете бути відокремлені в інформаційно незалежні потоки. Якщо розглядається поточний час, слід негайно відреагувати на інформацію, опубліковану в нижче перерахованих джерелах. З'ясуйте, хто був ініціатором, і підготуйте інформаційні контрзаходи. Якщо ви керівник компанії, зверніться до менеджера зі зв'язків з громадськістю та співробітника, який відповідає за антикризовий PR. У разі ретро-дослідження слід проаналізувати джерела-ініціатори, інформаційні повідомлення та їх однорідність, хто був зацікавлений у поширенні інформації. Зіставлення власного досвіду і розуміння ситуації з активними учасниками інформаційного удару може зміцнити або перетворити ваші версії щодо активності ваших конкурентів, недоброзичливців або соціального протистояння громадських ініціатив.»*

Опис звіту, що отримано за запитом користувача

Звіт містить первинний опис інформаційної ситуації: кількість знайдених публікацій, величину Атак Індексу.

Надається таблиця найбільших сплесків активності і дати, що їм відповідають, набираючи не менше значення ніж 30 з 100 можливих балів.

Інформаційна картина представляє собою графік кількості публікацій за

періоду що досліджується (*рис. 4*). Можна детально розглянути *«портрет»* запиту в інформаційному полі.

При наведенні на дату на лінії графіка, показується кількість публікацій за цей день.

При кліку на даті на графіку формується додатковий запит, який виводить ТОП-30 сюжетів за добу, повні тексти публікації із посиланнями на першоджерело, першу публікацію у серії сюжетів.

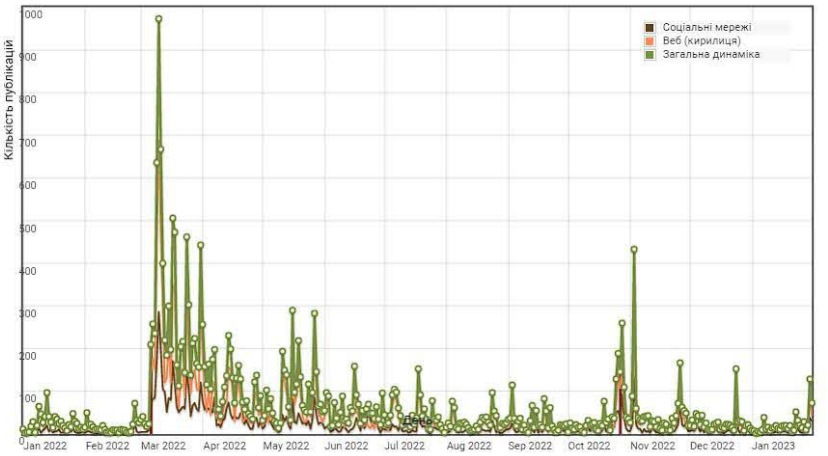

Рисунок 4. Інформаційна картка Атак Індекс

Сентимент аналіз

Представлено інформаційну динаміку за запитом з розподілом по позитивним (зелений колір) і негативним (червоний колір) публікаціям (*рис. 5*). Тональність визначається за допомогою машинного навчання. Не завжди наявність негативних індикаторів свідчить про негативний стан об'єкта дослідження. Можливо так, що ведеться дуже позитивна діяльність в умовах негативного оточення (війна, боротьба з корупцією тощо).

При наведенні на дату показується кількість позитивних або негативних публікацій за добу.

При натисканні мишкою на дату і обрану тональність формується додатковий запит, що показує приклад публікації із посиланням на першоджерело.

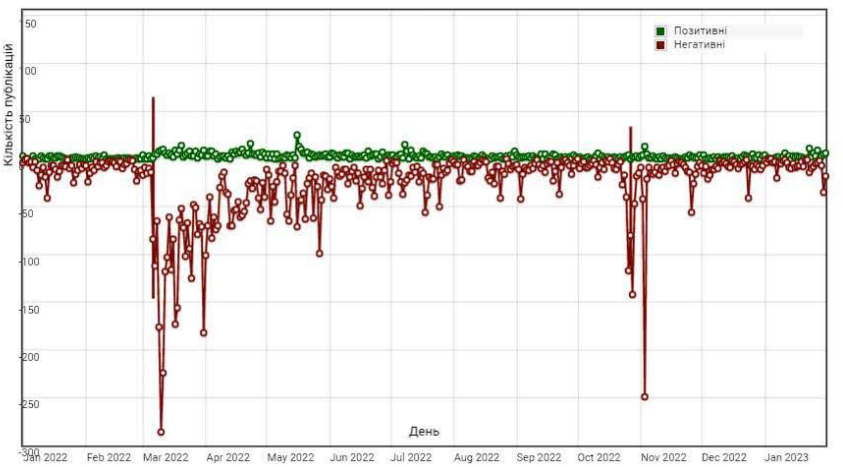

Рисунок 5. Сентимент аналіз Атак Індекс

Характеристики джерел

На основі Топ-20 джерел публікацій за весь період запиту система здійснює кількісний та якісний їх аналіз за різними характеристиками (*рис. 6, 7*).

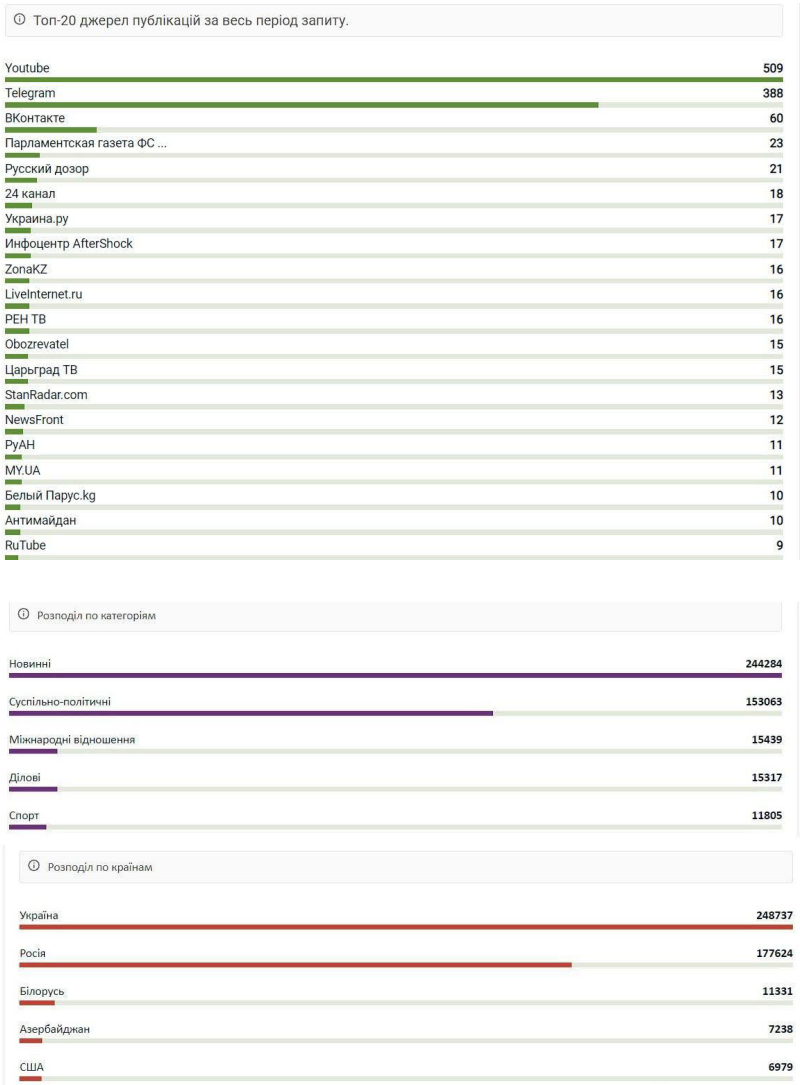

Рисунок 6. Кількісний аналіз джерел Атак Індекс

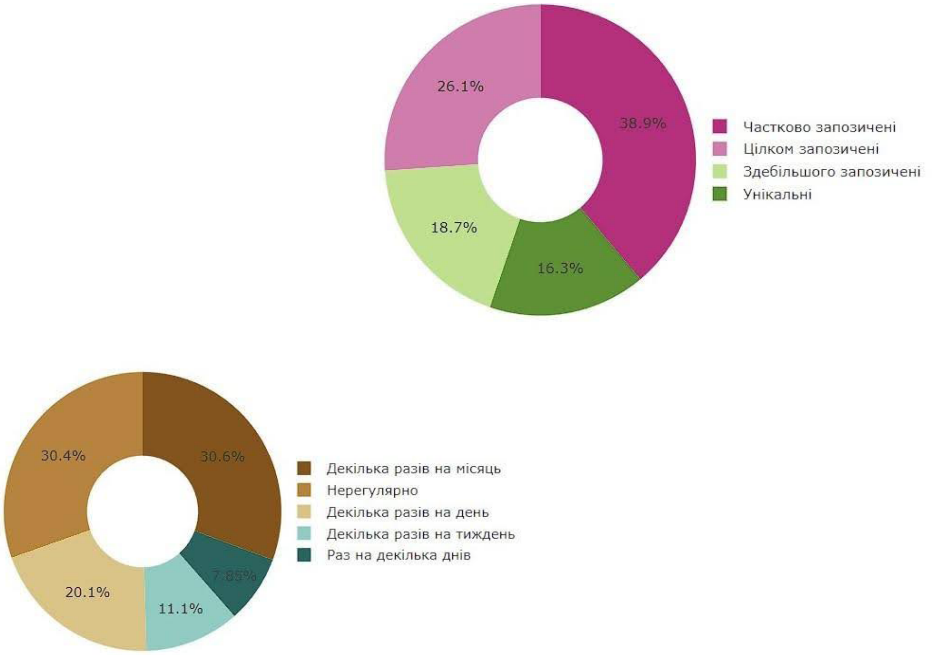

Рисунок 7. Якісний аналіз джерел Атак Індекс

Тренди

Активність об'єкта дослідження представлена графічно (*рис. 8*). Відхилення від середнього рівня кількості згадок об'єкта за період, що досліджується, представлені з прив'язкою до шкали часу. Максимальне відхилення відмічено жовтим кольором, низький рівень – зеленим. При наведенні курсору на графік можна бачити, на яку дату припадає відповідна інформаційна активність.

> За запитуваний період ми виявили ___ пік(ів) активності: *рррр.мм.дд.* На графіку вони вказані з прив'язкою до шкали часу.

Топ-20 джерел публікацій за дату максимальної інформаційної активності (рррр.мм.дд).

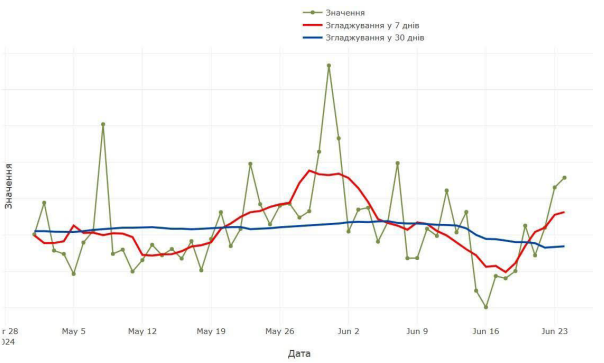

Рисунок 8. Активність об'єкта дослідження Атак Індекс

Інформаційні операції

Важливо знати ситуацію на досліджуваному часовому інтервалі та правильно планувати власну активність у відповідності до задіяних ресурсів можливих недоброзичливців. Підготовча фаза операції зазвичай пов'язана з залежними

від Ініціатора контент-майданчиками або спікерами. Подальший типовий інформаційний удар, як правило, задіює незалежні ресурси, що концентруються на області діяльності або підвищеному соціальному контакті.

Графік *«Інформаційні операції»* показує штучний вплив на потік інформації. Чим вище і більш насиченим є червоний сегмент хвильового графіка – тим більше ситуація навколо об'єкта дослідження відповідає шаблону *інформаційної операції (ІО)* (*рис. 9*).

> **Наприклад результат:** Система визначила, що *рррр.мм.дд* виявлено найбільше співпадіння шаблону інформаційної операції з величиною ІО = __ (0-100).

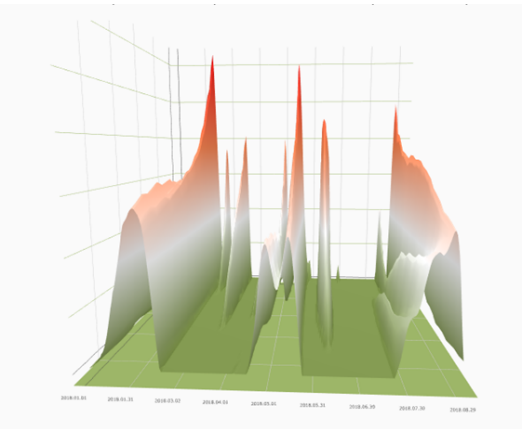

Рисунок 9. Графік «Інформаційні операції» Атак Індекс

Графік *«Контурна карта»* дозволяє в деталях розібратися в датах початку, тривалості та згасання виявлених штучних хвиль інформаційних операцій. Чим більш насиченим є червоний колір – тим більше ознак інформаційної операції (*рис. 10*).

Система аналізує наявність інформаційної операції тривалістю від 7 до 30 днів. При переміщенні курсора вертикально за датою можна побачити максимальне значення ймовірності збігу інформаційної динаміки з класичним шаблоном інформаційної операції.

Можна відстежувати максимальне значення (до 100) *параметра ІО*, це значення відповідає *кількості днів (К)*, протягом яких відбувалися основні фази операції.

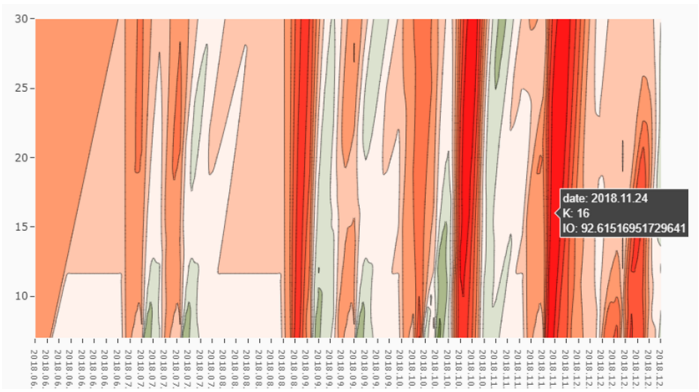

Рисунок 10. Графік «Контурна карта» Атак Індекс

Для дати *рррр.мм.дд*, яка найбільш імовірно збігається з шаблоном інформаційної операції, надається до 5 сюжетів та відповідних їм ресурсів розповсюджувачів інформації

Зв'язки джерел

Для зручності зв'язки між ресурсами зображено у вигляді павутини (*рис. 11*). Павутина зв'язків показує взаємозалежність (*наприклад, передрук чи наявність посилань*) 20 найбільш значущих об'єктів інформаційного сплеску або операції в розраховану дату. Радіус кола джерела залежить від кількості публікацій.

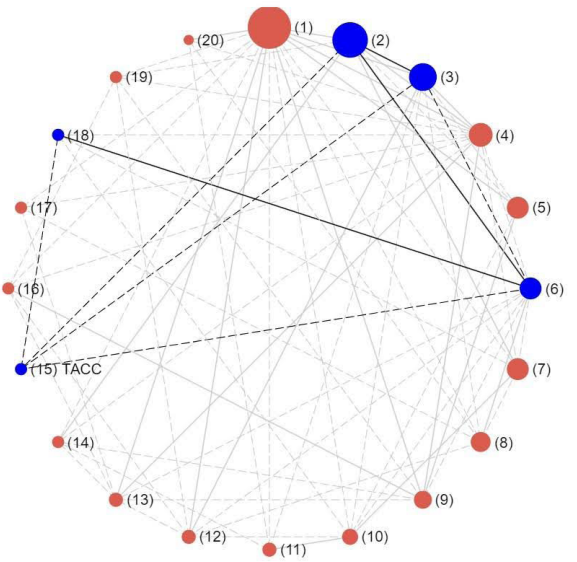

Рисунок 11. Павутина зв'язків Атак Індекс

При активації курсора на сегмент синього кольору показується зв'язок з іншими. Суцільними лініями показуються найсильніші зв'язку між джерелами.

Розділ представляє топ-20 джерел за максимальною величиною індексу атаки. Звертаємо увагу, що це топ-джерела на період максимального інформаційного сплеску або операції, а не за весь часовий проміжок, на якому проводилося дослідження (відповідний графік є в першому розділі звіту).

Стабільність та прогноз

Розділ надає інформацію про стабільність ситуації. Значення коефіцієнта Херста (*рис. 12*), близькі до 0,5, говорять про хаос процесу. Чим ближче значення до 1 – тим стабільніший процес, майбутнє повторює минуле. Різкі стрибки коефіцієнта свідчать про наявність дуже різних неоднорідних процесів. Можливо, слід збільшувати досліджувані часові проміжки – для кращого розуміння тенденцій в активності досліджуваного об'єкта.

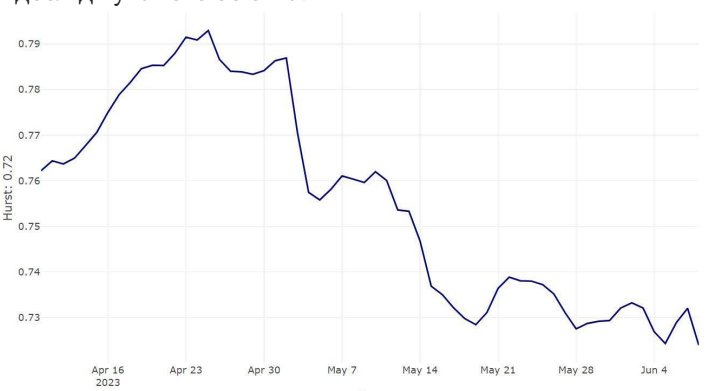

Рисунок 12. Значення коефіцієнта Херста Атак Індекс

Прогнози розвитку інформаційної динаміки запиту

Для наявних часових рядів динаміки публікацій розміром 200 діб, можна говорити про подальший прогноз на 20 днів з точністю 90 %.

Лінгво-кореляційний метод

Прогноз здійснюється лінгвістичним методом прогнозування, який використовується для обробки природної мови, зокрема для передбачення наступних слів у висловлюванні, якщо відомі всі попередні. Прогноз відображається графічно (*рис. 13*). При цьому вважається, що умовна ймовірність появи наступного слова залежить від попередніх слів і їх послідовностей. Для прогнозування часового ряду, як відомо, також використовується припущення, що ймовірність і його значення визначаються попередніми значеннями.

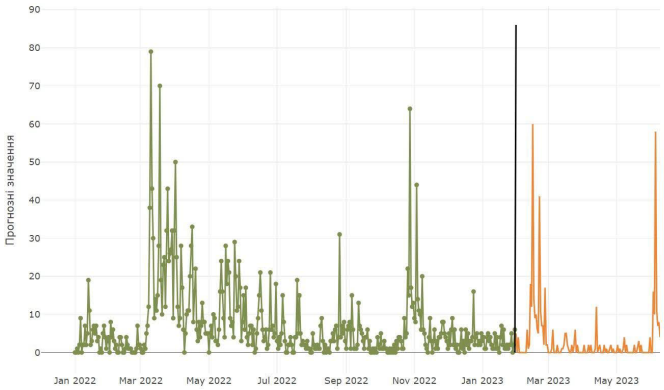

Рисунок 13. Візуалізація прогнозу Атак Індекс

Метод визначення кризової ситуації

Метод, запропонований Д. Сорнетте, базується на аналізі регулярності ринкових цін на товарних та фондових ринках до кризи. Основна ідея цього методу випливає з аналізу фінансових часових рядів напередодні кризи і полягає у тому, що до кризи ці значення характеризується зростанням за степеневим законом, ускладненим періодичними коливаннями, що сходяться до критичної точки, коли ймовірність колапсу досягає максимального значення (*рис. 14*).

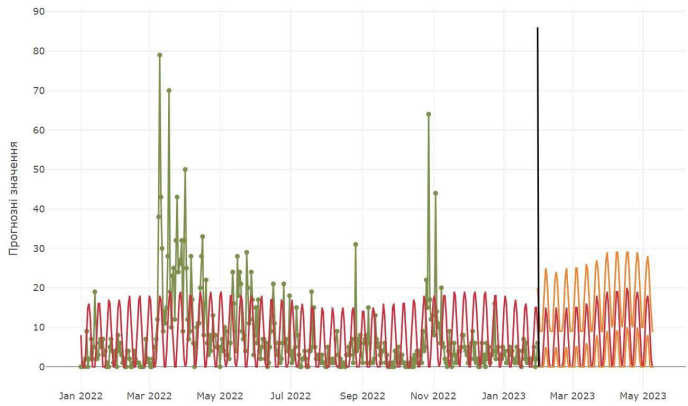

Рисунок 14. Візуалізація кризової ситуації Атак Індекс

Метод визначення тренду розвитку ситуації

Поліноміальна регресія моделює лише розвиток тренду складової часового ряду (*рис. 15*). Історичний ряд даних розкладається за методом найменших квадратів у відповідності із заданим ступенем поліному. Поліноміальна регресія може застосовуватися у математичній статистиці при моделюванні трендових складових процесів, що розвиваються у часі.

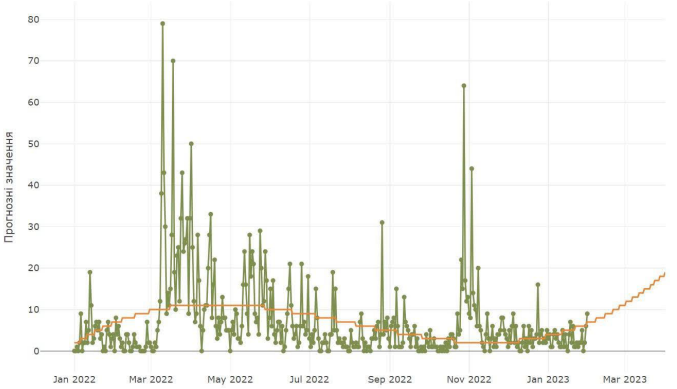

Рисунок 15. Візуалізація тренду розвитку ситуації Атак Індекс

Метод визначення періодичних процесів

Метод розкладання у ряди Фур'є дозволяє знайти періодичні форми процесів (*рис. 16*), наприклад відображення редакційних політик джерел у часі за застосованим запитом. За отриманою апроксимованою формулою відбувається подальше прогнозування.

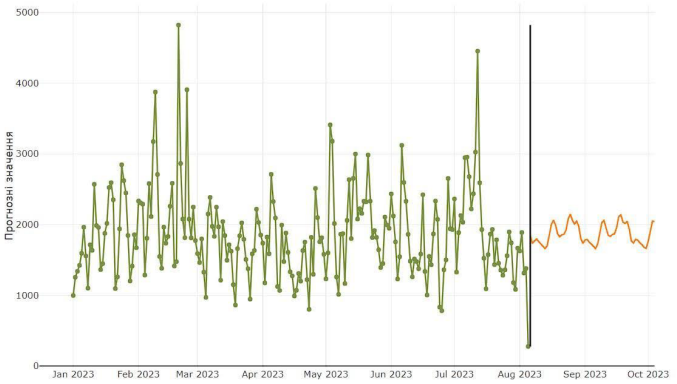

Рисунок 16. Візуалізація періодичних процесів Атак Індекс

ЦИТУВАННЯ

Наведено всі фрагменти прямої мови, що присутні у повідомленнях, які відповідають запиту. У таблиці, рядки відповідають фрагментам появи прямої мови в окремих повідомленнях. Кожний рядок містить таку інформацію: автор фрагменту, саме висловлювання, яке можна цитувати, день та час відповідного повідомлення і його адреса в мережі (URL).

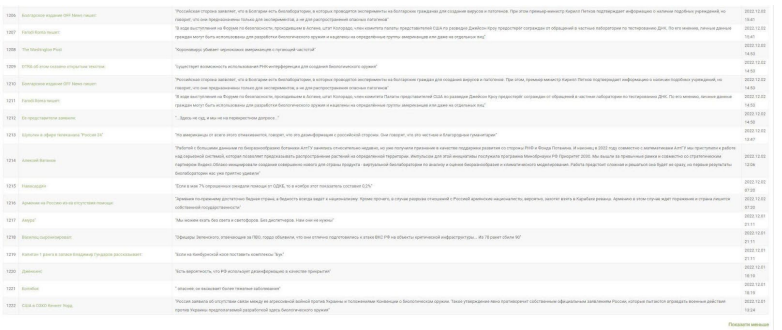

Рисунок 17. Візуалізація цитувань Атак Індекс

ТЕГИ

Опція Теги надає відповідну кількісну інформацію щодо усього масиву тегів, знайдених за запитом і помічених символом *«#»* (*рис. 18*). Більшість тегів зазвичай присутні у соціальних мережах, але можуть бути використані і на інших ресурсах. Список тегів відсортовано за частотою використання.

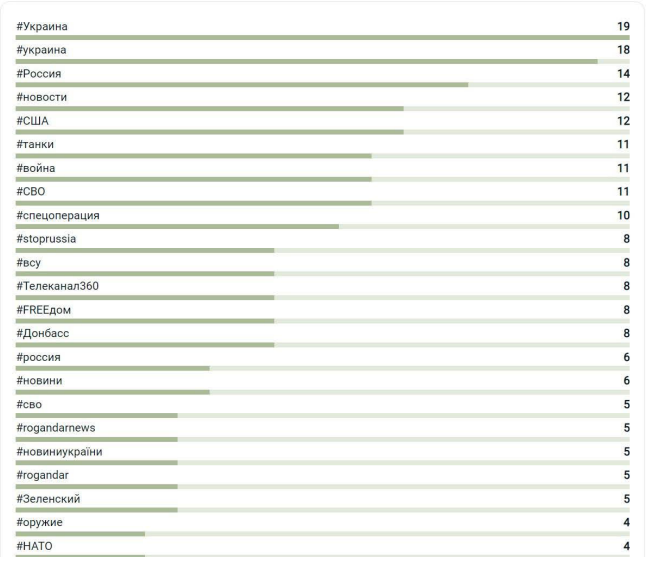

Рисунок 18. Теги знайдені за запитом Атак Індекс

Портрети

У розділі користувач може побачити лист іменних сутностей – фізичних чи юридичних осіб, які згадувались у повідомленнях, що відповідають його запиту (*рис. 19*). На основі цих сутностей будується граф, на вузлах якого відображаються графічні зображення – портрети персон, або позначки організацій, якщо вони відомі системі. Активуючи курсор на назві джерела синім кольором показується зв'язок для вибраного джерела з іншими.

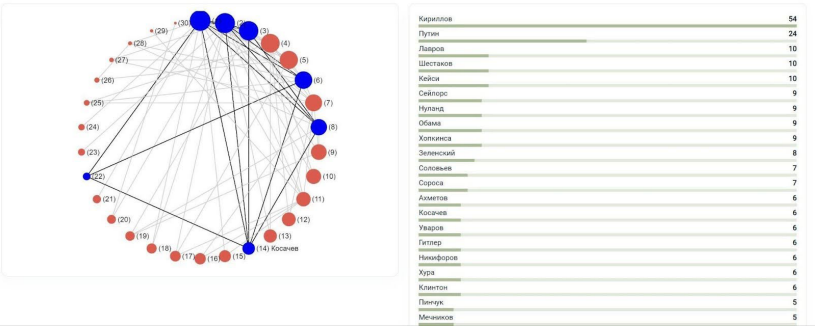

Рисунок 19. Портрети сутностей та їх зв'язки

ГЕО

У режимі *«Гео»* користувач може побачити основні географічні назви (переважно міста), які присутні в повідомленнях, що відповідають його запиту (*рис. 20*). Виводиться перелік цих географічних назв і шкала частоти появи назв у повідомленнях.

Вибравши зі списку геолокацію можна перейти у режим пошуку за первинним запитом, з уточненням цієї географічної назви.

Рисунок 20. Геолокація інформаційної активності

ВИСНОВОК

Сучасні інструменти OSINT, розроблені з урахуванням національного контексту, демонструють здатність поєднувати гнучкість збору даних із структурованою аналітикою, що відповідає оперативним і стратегічним потребам сектору безпеки. Їхнє застосування дозволяє не лише автоматизувати процеси моніторингу відкритих джерел, а й виявляти приховані зв'язки, тенденції та ризики у багатовимірному інформаційному середовищі.

Ключовими перевагами таких рішень є:

- *модульність і адаптивність* до різних типів задач – від реагування на інциденти до стратегічного прогнозування;
- *інтеграція з етичними стандартами* та можливість формування прозорих процедур перевірки даних;
- *підтримка міжвідомчої співпраці*, що сприяє синхронізації дій у складних інформаційних операціях;
- *візуалізація та пояснюваність результатів*, що підвищує довіру до аналітики серед прийняття рішень.

У контексті трансформації української аналітичної екосистеми, подібні інструменти відіграють критичну роль у формуванні стійкої, технологічно озброєної та етично вмотивованої культури OSINT. Їхнє впровадження – це не лише технічний прогрес, а й крок до глибшого розуміння інформаційного простору як середовища для захисту, діалогу та стратегічного розвитку.

РОЗДІЛ 15

ЗАСТОСУВАННЯ ШІ У ЗБОРІ ТА АНАЛІЗІ ЦИФРОВОГО СЛІДУ

Володимир ЛОЗОВИЙ
Дмитро ХУДЕНКО

У сучасному світі, де середньостатистична людина проводить в інтернеті близько 7 годин на день та залишає значний цифровий слід, використання інструментів штучного інтелекту для аналізу стає ефективним і доцільним підходом. Збір і аналіз цифрового сліду профілю вручну може займати кілька днів, тоді, як із застосуванням ШІ, цей процес значно пришвидшується.

В Україні одним із найбільш комплексних рішень у цій сфері є система **BigDataPeople2** компанії **Artellence**, яка дозволяє працювати з відкритою інформацією із соціальних мереж, державних реєстрів, професійних сайтів, ресурсів з пошуку роботи та маркетплейсів, що обробляється з 2006 року.

Джерелами даних є загальнодоступні (публічні) дані, які користувачі добровільно розмістили у відкритому доступі в мережі Інтернет, зокрема:

- *соціальні мережі,*
- *державні реєстри,*
- *професійні ресурси,*
- *сайти з пошуку роботи,*
- *маркетплейси,*
- *а також веб-сайти та публікації, доступні через пошукові системи.*

Загальний обсяг даних з 2006 року: інформація про понад 3 мільярди профілів, 100 мільярдів взаємодій, 5 мільярдів фотографій отримані з публічних джерел, відповідно до чинного законодавства.

Продукт включає 6 спеціалізованих модулів (*рис. 1*):

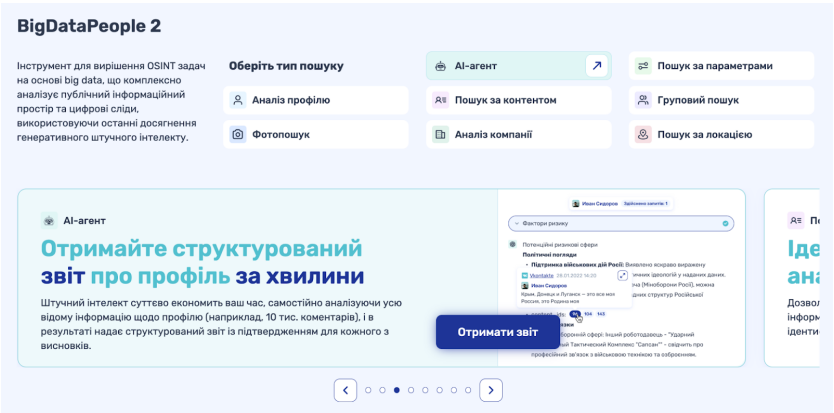

Рисунок 1. Основні модулі продукту BigDataPeople 2

– *Аналіз профілю* – дослідження цифрового сліду користувача, виявлення ризиків, агрегація інформації.
– *AI-агент* – використання провідних великих мовних моделей (LLM) для автоматичного аналізу великих обсягів інформації та формування структурованого звіту з посиланнями на джерела.
– *Фотопошук* – пошук фотографій з профілів та інформаційних ресурсів, на яких присутнє надане обличчя.
– *Пошук за контентом* – аналіз інформаційних ресурсів, дописів і коментарів, з можливістю пошуку за ключовими словами.
– *Пошук за локацією* – аналіз контенту, що був опублікований у заданому радіусі від визначеної точки.
– *Аналіз компанії* – дослідження інформації про юридичних осіб у реєстрах, ЗМІ та соціальних мережах.

Ключовою перевагою продукту є автоматизація аналізу великих обсягів інформації із застосуванням власних алгоритмів штучного інтелекту та технологій провідних розробників великих мовних моделей. Продукт не лише дозволяє відшукати інформацію, а й поєднує дані з декількох ресурсів, визначає ключові фактори, що потребують уваги, та надає у використання зручні фільтри й автоматизації для швидкого аналізу інформації.

BigDataPeople2 працює виключно з публічно доступною інформацією, яку користувачі добровільно розмістили у відкритому доступі, або яка є доступною через відкриті державні реєстри, професійні сайти, соціальні мережі та інші загальнодоступні ресурси.

Розглянемо декілька основних частин продукту.

Аналіз профілів користувачів

Для використання продукту, користувач має мати правові підстави та право на аналіз даних профілю, що досліджується.

Для пошуку профілів продукт дозволяє використовувати різні дані, що містяться у соцмережах або на інших ресурсах: фото, номер телефона, ім'я, нікнейм, навчальний заклад, посилання на профіль тощо (*рис. 2*).

Важливо зазначити, що результатів може бути кілька, і вони можуть включати профілі з різних соцмереж. Це – значна перевага, оскільки пошук різних сторінок одного користувача зазвичай є трудомістким поцесом: не всі підписуються однаково, існує безліч варіантів написання імені.

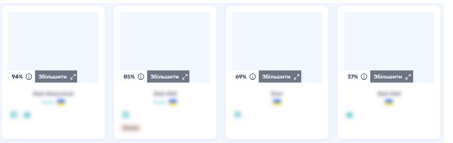

Рисунок 2. Аналіз профілю BigDataPeople 2

Можливості роботи з фото

Під час пошуку за фото алгоритми ідентифікують профіль у 95% випадків, за умови, що фото профілю наявні в соцмережах, а якість вхідного зображення є достатньою.

Попри функцію пошуку профілю за фотографією, продукт також здатен здійснювати пошук обличчя профілю на всіх відомих сторінках соцмереж – на фотографіях інших профілів, а також на сторінках інформаційних ресурсів, лідерів думок, спільнот і груп (*рис. 3*).

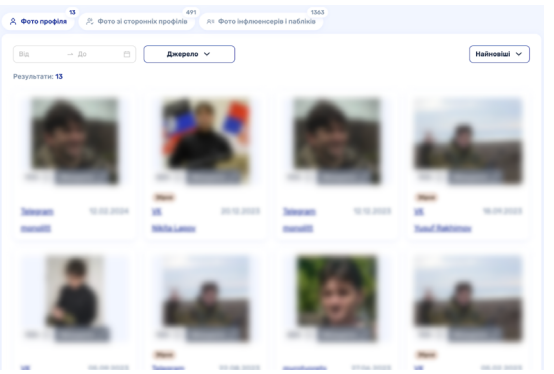

Рисунок 3. Можливості роботи з фото BigDataPeople 2

Також продукт розпізнає на фото військову форму, зброю, техніку та дозволяє швидко знаходити подібні зображення (*рис. 4*).

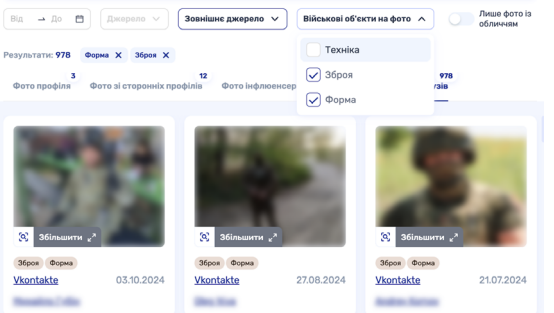

Рисунок 4. Можливості розпізнавання на фото BigDataPeople 2

Аналіз характеристик профілів

Після вибору профілю здійснюється його аналітична обробка, яка охоплює контент, зображення та соціальні зв'язки. Продукт також надає можливість автоматично виявляти ознаки інформації, які можуть бути корисними для подальшого аналізу, зокрема:

- *публічні зв'язки профілю з особами, що перебувають на території рф;*
- *взаємодію профілю з контентом, що стосується російської політики;*
- *згадки про участь у військовій діяльності або наявність відповідних атрибутів в контенті;*
- *ознаки іншої ризикової тематики в контенті профілю.*

Усі виявлені ознаки є предметом подальшої професійної оцінки аналітиком. Система не формує самостійних висновків про профіль. Виявлені характеристики лише свідчать про наявність взаємодії профілю з відповідним контентом і не є підтвердженням особистих поглядів або переконань власника профілю. Ці ознаки можуть використовуватися для формулювання гіпотез, які потребують подальшого аналізу та перевірки.

Автоматизований аналіз за допомогою AI-агента

Як вже було зазначено раніше, контент, опублікований профілем, може слугувати джерелом для аналітичних припущень щодо поглядів та ставлення його автора до певних тем.

Тому для більш ґрунтовної перевірки, продукт пропонує два підходи до аналізу контенту, створеного профілем:

- ручний аналіз за допомогою зручних фільтрів у продукті;
- автоматичний аналіз за допомогою вбудованого AI-агента.

AI-агент самостійно аналізує контент і генерує звіт, що включає всю інформацію про те, про що писав профіль, що він вподобав чи поширив, а також аналізує вибірку його оточення.

Наприклад, за допомогою запиту *"Соціальна взаємодія"* ШІ може виявляти контент, пов'язаний із соціально чутливими темами, для подальшого аналізу користувачем. Інтерпретація результатів завжди залишається за аналітиком. До звіту додаються посилання на джерела, які доступні для перегляду, що дозволяє перевірити коректність отриманих результатів. Це важливо, оскільки при аналізі із застосуванням ШІ-інструментів завжди існує ймовірність похибок.

При оцінці активності профілю користувача особливо корисним є аналіз за допомогою ШІ, оскільки він охоплює публічно доступні джерела, в яких профіль міг залишати контент.

Іноді спостерігаються випадки, коли один і той самий профіль у різних соціальних мережах демонструє відмінну активність – наприклад, може підтримувати проукраїнську позицію в одній мережі, водночас висловлюючи протилежні думки в іншій.

Відповідальність за правомірність збору, обробки та використання даних під час роботи з продуктом BigDataPeople2 несе безпосередньо користувач. Компанія надає інструмент для аналітики, проте не здійснює перевірку законних підстав використання інформації в кожному окремому випадку.

ВИСНОВОК

Інтеграція спеціалізованих інструментів OSINT у національну аналітичну практику відкриває нові горизонти для системного, етичного та оперативного

опрацювання відкритих даних. Подібні рішення демонструють здатність поєднувати глибину алгоритмічного аналізу з гнучкістю користувацьких сценаріїв, забезпечуючи ефективну підтримку як для оперативних служб, так і для стратегічного планування.

Серед ключових характеристик таких інструментів:

- *спроможність до багатоканального збору та кореляції даних*, що дозволяє виявляти складні інформаційні патерни;
- *вбудовані механізми перевірки*, фільтрації та класифікації, які підвищують якість і достовірність аналітичних висновків;
- *можливість адаптації до локальних контекстів*, включно з мовними, правовими та культурними особливостями;
- *підтримка прозорої документації та навчальних сценаріїв*, що сприяє масштабуванню знань і формуванню спільної аналітичної культури.

У часи інформаційної турбулентності, подібні інструменти стають не просто технологічними рішеннями, а інституційними опорами – вони формують нову етику роботи з відкритими джерелами, зміцнюють довіру до аналітики та дозволяють діяти на випередження в умовах гібридних загроз.

РОЗДІЛ 16

АНАЛІТИЧНІ СИСТЕМИ ДЛЯ ПЕРЕВІРКИ КОМПАНІЙ ТА ПІДПРИЄМЦІВ НА ОСНОВІ ВІДКРИТИХ ДАНИХ

Анатолій ПЯСЕЦЬКИЙ
Дмитро ХУДЕНКО

Продукти YouControl стали одними із незамінних інструментів для розслідувань, верифікації даних та пошуку втраченої інформації (*рис. 1*). Їх можливості дозволяють ефективно аналізувати відкриті дані, мінімізувати ризики та приймати обґрунтовані та виважені рішення. Розглянемо два основі продукти.

Система YouControl є самодостатнім та потужним інструментом для збору, аналізу та перевірки інформації про фізичних осіб, фізичних осіб-підприємців і юридичних осіб. Завдяки комплексним аналітичним інструментам, скоринговим моделям та рішенням на основі штучного інтелекту, вона не лише забезпечує доступ до важливих даних, а й формує готові висновки для оперативного прийняття рішень.

Важливою перевагою YouControl є каталог компаній, судових рішень і декларацій, який виконує роль архіву даних. Це не лише спрощує доступ до важливої інформації, а й гарантує її збереження, запобігаючи видаленню чи маніпуляціям в офіційних джерелах.

Окремо варто відзначити суспільну значущість платформи. Компанія дотримується чіткої громадянської позиції, надаючи безкоштовний доступ громадським діячам, активістам та антикорупціонерам. Це сприяє підвищенню прозорості, боротьбі з корупцією та розвитку відкритого суспільства.

Система YouControl – це українська аналітична система для комплаєнсу, аналізу конкурентів, ділової розвідки та розслідувань.

Джерелами даних є українські державні реєстри, інші відкриті дані, матеріали журналістських розслідувань, аналітичні статті, іноземні державні реєстри та інші джерела, інформація з яких не обмежена у використанні та обробці. Система

містить понад 200 українських джерел (YouControl) та більше 300 іноземних (YC World).

Також до системи звертаються у випадках, коли не завантажуються державні реєстри, наприклад, із технічних причин або у випадку збройної агресії з боку рф. Каталоги компаній та судових рішень стали резервними даними і стримуючим фактором від видалення або фальсифікації документів.

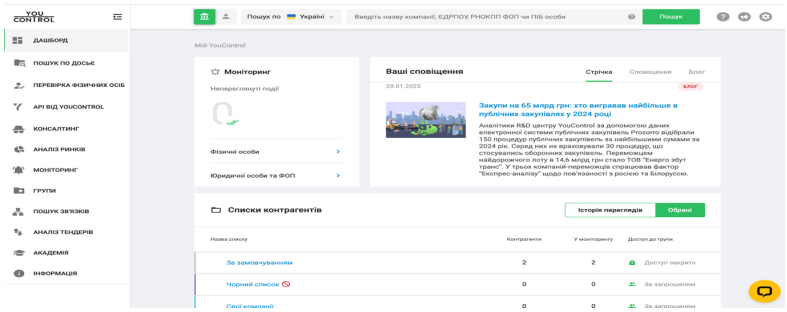

Рисунок 1. Загальний вигляд стартової сторінки з панеллю керування

YOUCONTROL

Щоб оцінити функціонал і можливості аналітичної системи YouControl, візьмемо за об'єкт дослідження ПРАТ «Телеканал Інтер» та бізнес-партнерів Дмитра Фірташа, а також складемо детальне досьє на нього.

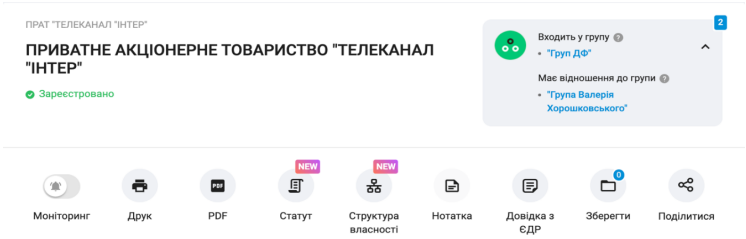

Рисунок 2. Результат пошуку за вказаним критерієм - ПІБ посадової особи

Для початку знайдемо всі згадки за критерієм *«Фірташ Дмитро Васильович»* (*рис. 3*). Водночас система дає можливість здійснювати пошук за рядом інших критеріїв (ідентифікаторів). Це може бути назва юридичної особи, адреса реєстрації, код ЄДРПОУ або номер ІПН, ПІБ уповноважених осіб тощо. Також можна конкретизувати результат пошуку, вказавши регіон, стан суб'єкта або навіть вид діяльності.

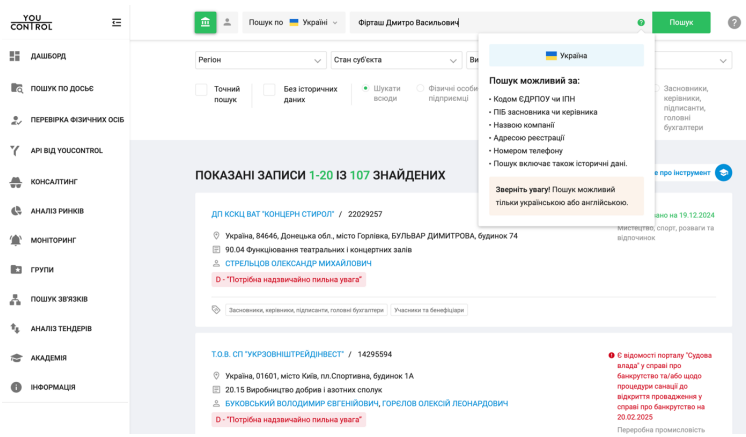

Рисунок 3. Навігаційні кнопки в досьє

Серед результатів пошуку переходимо на той, що нас цікавить і отримуємо повне, вичерпне досьє, що актуальне на момент запиту. Його можна відразу ж завантажити, надіслати на електронну пошту, завантажити або роздрукувати.

Система YouControl автоматично перевіряє інформацію, аналізує майже 600 показників і дає консолідований експрес-аналіз, а також вказує на фактори експрес-аналізу, що наявні у компанії. В даному випадку ми бачимо, що до компанії потрібна надзвичайно пильна увага.

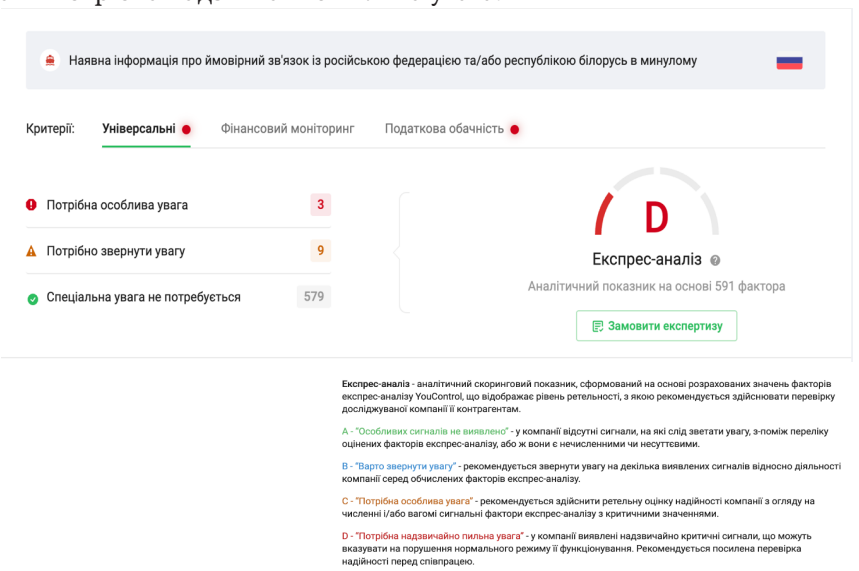

Рисунок 4. Експрес-аналіз контрагента з оцінкою та переліком наявних ризик-факторів

Для детального опрацювання кожного ризик-фактору є можливість розкрити весь перелік і оцінити які наслідки від співпраці можуть бути. В прикладі з ПРАТ «Телеканал *«Інтер»* є стоп-фактори – санкції до самого суб'єкта господарювання, санкції до посадової особи та історичні зв'язки з рф.

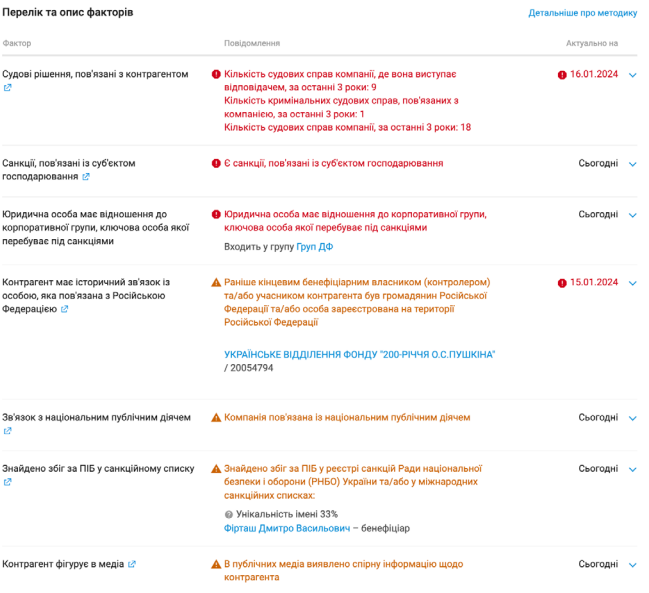

Рисунок 5. Перелік та опис факторів

Основна цінність системи в її аналітичних інструментах, що спрощують перевірку та прискорюють аналіз даних. З недавнього часу є опція генерування за запитом користувача звіту за допомогою штучного інтелекту (*рис. 6*).

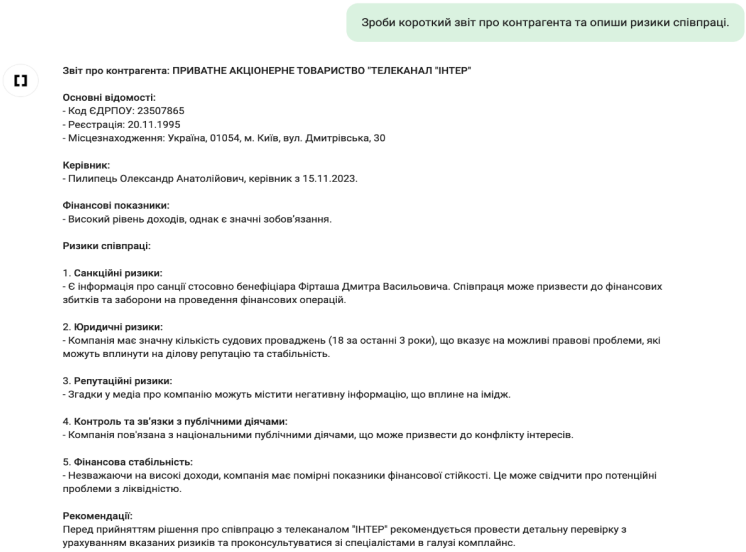

Рисунок 6. Звіт про контрагента, згенерований за допомогою AI

Якщо необхідно провести детальний аналіз контрагента, відкриваємо розширене досьє компанії, структуроване за тематичними вкладками для зручності навігації. Кожна вкладка містить інформацію із зазначенням джерела її походження.

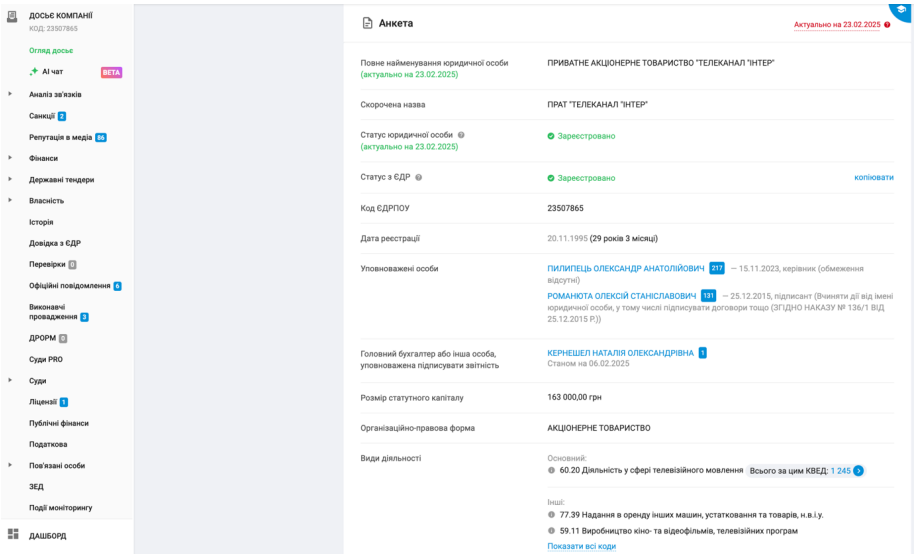

Рисунок 7. Досьє компанії та навігаційна панель

І в даному випадку система піклується про користувача – навпроти назви вкладки вказує на наявність та кількість документів, що міститься в розділі (наприклад, згадка в 2-х санкційних документах або згадка в 86-ти публікаціях засобів масової інформації). Крім того, більшість розділів оснащені вбудованими аналітичними інструментами, які прискорюють обробку великих обсягів даних, мінімізують вплив людського фактора та автоматизують рутинні процеси (*рис. 8-11*).

Рисунок 8. Приклад аналізу репутації контрагента в медіа

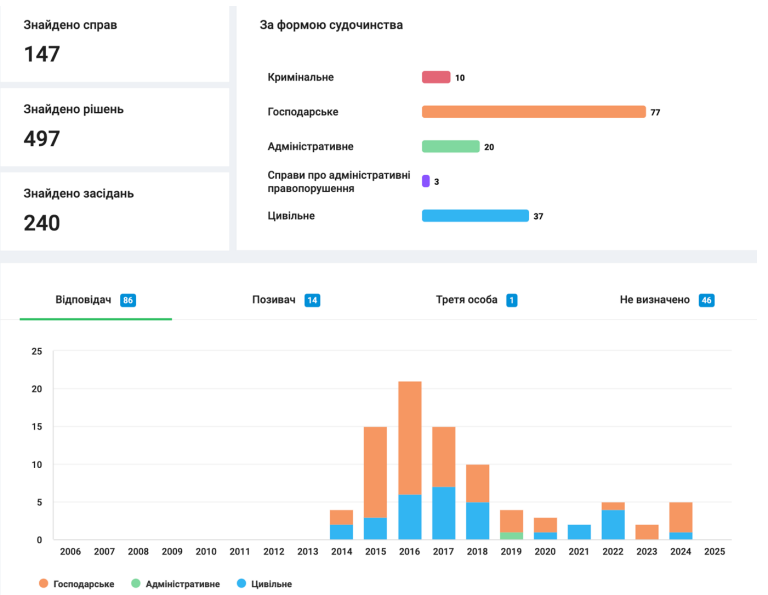

Рисунок 9. Приклад аналізу судових документів, що стосуються контрагента

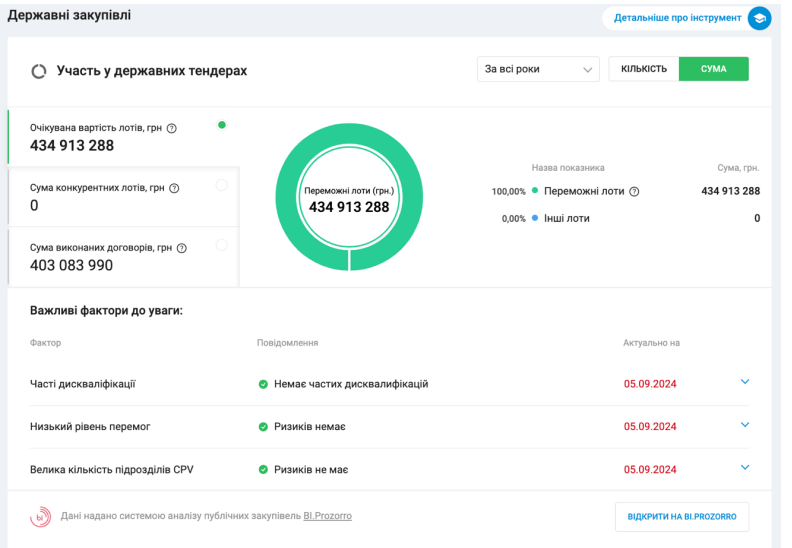

Рисунок 10. Приклад аналізу активності контрагента у державних закупівлях

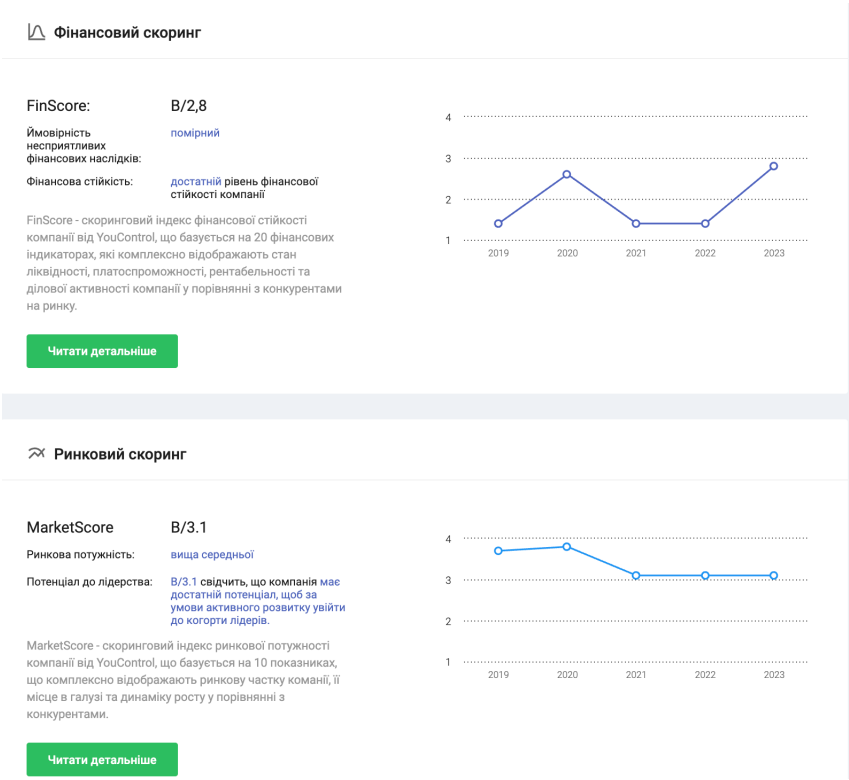

Рисунок 11. Приклад аналізу фінансової стійкості та ринкової потужності

Для повноти аналізу та формування звіту важливо дослідити коло пов'язаних компаній та осіб. Такий функціонал передбачений в розділі *«Аналіз зв'язків»*. Система виявляє існуючі та історичні зв'язки за 10 різними типами, будує граф та дає можливість розкривати обрані вузли і заглиблюватися у структуру юридичної особи (*рис. 12*).

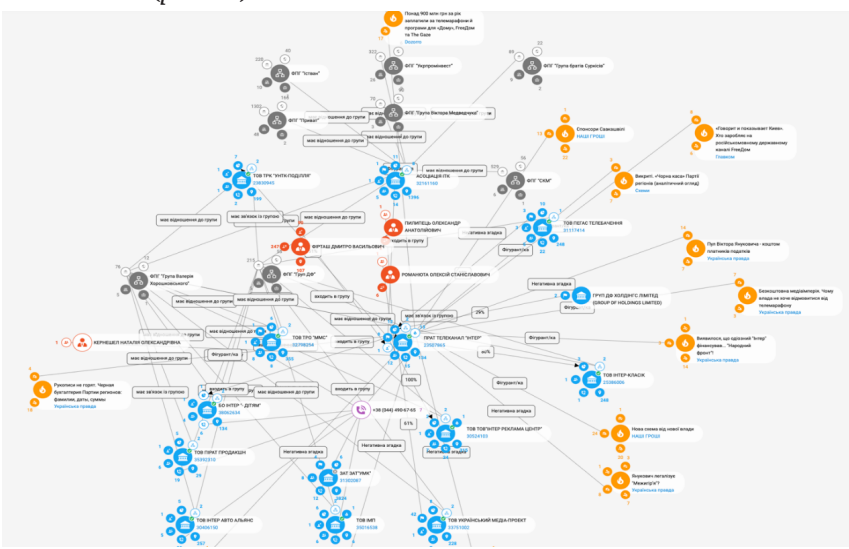

Рисунок 12. Приклад схематичного зображення зв' язків контрагента

Разом із цим інструментом коло афілійованих осіб та компаній може розкрити приналежність компанії до групи компаній, де також можуть бути вказані

позначки щодо пов'язаності фінансово-промислової групи до підсанкційних осіб, осіб, які мають статус національних публічних діячів (*рис. 13*), а також копія останнього актуального документа схематичного зображення структури власності (*рис. 14, 15*).

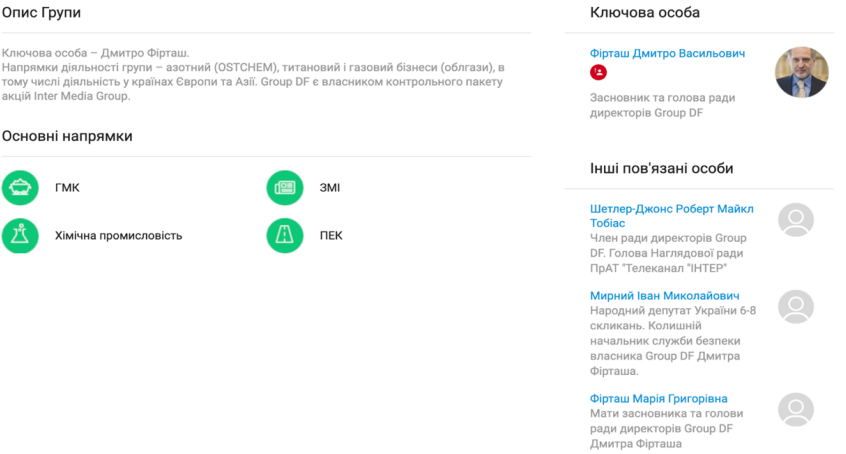

Рисунок 13. Приклад опису групи компаній

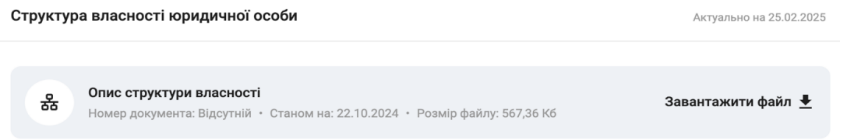

Рисунок 14. Запит на структуру власності

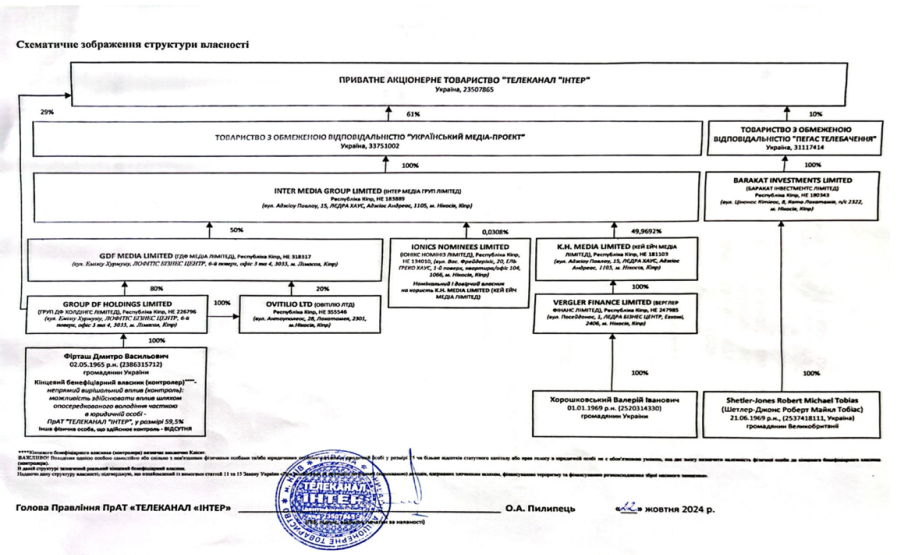

Рисунок 15. Зразок документа зі схематичним зображенням структури власності

Комплексне дослідження контрагента обов'язково має включати детальний аналіз та перевірку уповноважених осіб за їхніми ПІБ. З цією метою в окремому модулі *«Перевірка фізичних осіб»* вкажемо ПІБ кінцевого бенефіціарного власника – Фірташ Дмитро Васильович та здійснимо пошук (також додатково можна вказати і інші ідентифікатори – дату народження, РНОКПП, номер паспорта громадянина України чи документа про освіту (*рис. 16*). Але варто пам'ятати, що

при перевірці фізичної особи основним ідентифікатором є ПІБ особи і система вказує на унікальність і можливі збіги, групуючи їх за регіоном. Водночас, вказаний код РНОКПП чи дата народження можуть конкретизувати інформацію лише в деяких реєстрах, наприклад показати пов'язаний ФОП або вказати на виконавчі провадження. А паспорт громадянина України перевіряється лише на збіг з номерами викрадених, втрачених недійсних документів).

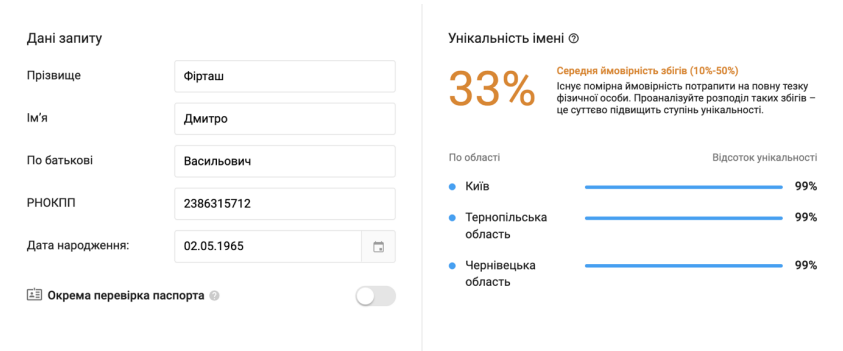

Рисунок 16. Зразок заповнення пошукового запиту по фізичній особі

Для зручної навігації вся структура досьє і тематичні вкладки виконані в тому ж стилі, що і досьє на юридичну особу. А логіка подачі інформації від загального до конкретного дозволяє вивчити найдрібніші деталі. У прикладі з об'єктом дослідження ми додатково виявили ще ряд важливих сфер обачності – велику кількість судових справ, обтяження рухомого майна та згадку особи в санкційних списках України та Великобританії.

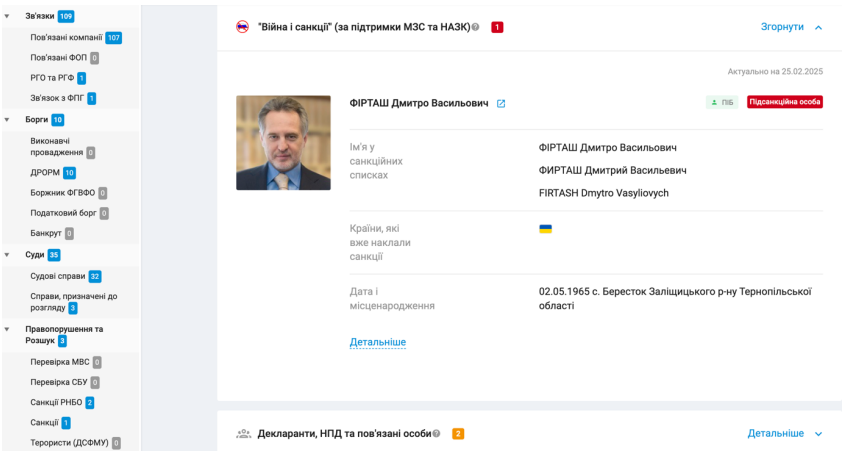

Рисунок 17. Зразок досьє на фізичну особу

YOUCONTROLWORLD

Що робити, коли з'являються кейси, в яких треба розширити географію перевірки чи пошуку? Наприклад, уповноважена особа української компанії-резидент України – є також уповноваженою особою компанії, зареєстрованої в іншій юрисдикції. Або взагалі необхідно здійснити перевірку іноземної компанії? В такому випадку варто скористатися інструментом для міжнародного пошуку та візуалізації бізнес-зв'язків **youcontrol.world**.

YouControlWorld – це та система, яка дозволить зробити додаткові розслідування по нерезидентам (*рис. 18*). Допоможе встановити інші зв'язки учасників нерезидентів, візуалізує *«токсичні»* зв'язки у вигляді зв'язків з країнами-агресорами, чи країнами-партнерами країн-агресорів, зв'язки з підсанкційними

особами, зв'язки з національними публічними діячами. Додатково завдяки *«World»* можна зробити власну візуалізацію своїх розслідувань, а також ділитись цією інформацією з іншими.

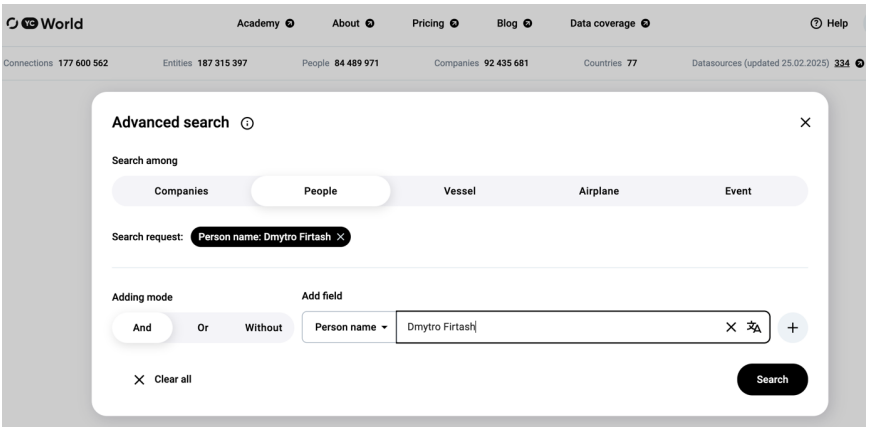

Рисунок 18. Загальний вигляд стартової сторінки youcontrol.world.

Інструмент дає можливість здійснювати пошук за різними ідентифікаторами (компанія, особа, яхти чи літаки) а також комбінувати їх між собою, уточнюючи критерій пошуку.

Для прикладу візьмемо прізвище та ім'я об'єкта попереднього дослідження та виявимо якими даними можна ще збагатити дані. Для цього в пошуковій стрічці напишемо прізвище та ім'я латинськими літерами.

За результатами виконання пошукового запиту є можливість конкретизувати отриману інформацію, вказавши окремо країну, яка нас цікавить, джерело цих даних, адресу реєстрації або навіть дату народження особи.

Окремо винесемо отримані результати на граф та миттєво отримаємо схематичне зображення зв'язків особи з іншими особами чи компаніями (*рис. 19*). Важливим є те, що на одному графі можна розмістити різні типи зв'язків. Також біля кожного вузла буде вказано до якої юрисдикції він відноситься.

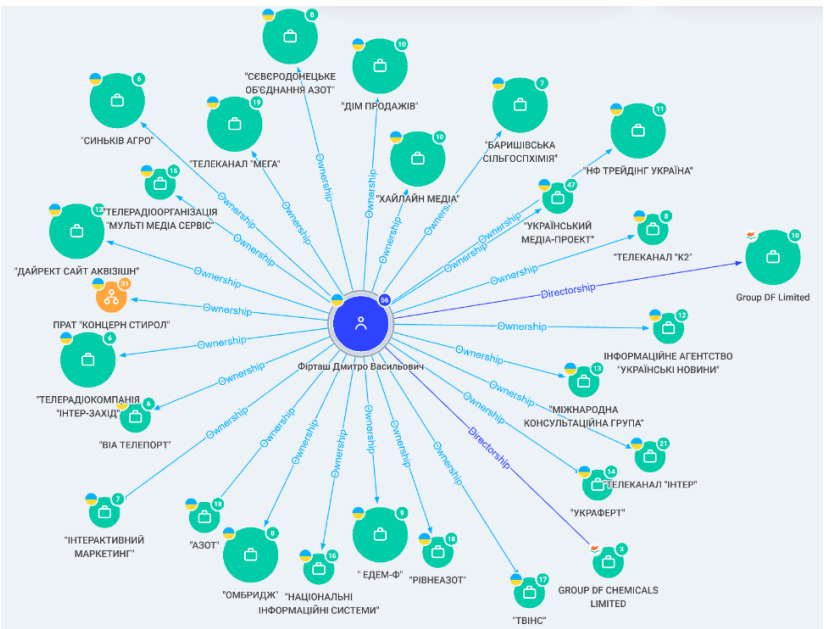

Рисунок 19. Результат пошуку за критерієм прізвище та ім'я

Разом із тим, система аналізує іноземні реєстри на наявність ризикових факторів таких як іноземні санкції чи зв'язок з російською федерацією (*рис. 20*).

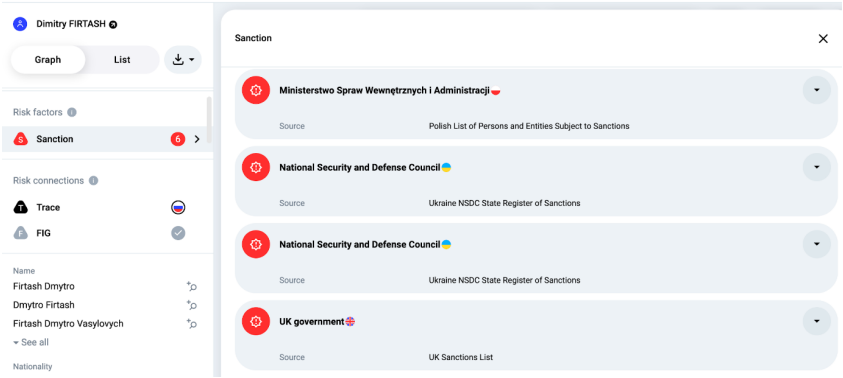

Рисунок 20. Аналіз ризикових факторів та зв'язків

Даний модуль дозволяє не лише встановити бізнес-зв'язки, виявити афілійованість з іноземними компаніями чи перевірити контрагента на ризик, а і ознайомитися з історичними ролями чи попередніми посадами фізичної особи або навіть збагатити дані важливою інформацією, як от адреси проживання, реєстраційні номери чи номери інших документів, дату народження чи номер телефону або посилання на персональний сайт.

Окрім вище вказаної інформації в системі YouControl.World зібрана найбільша база національних публічних діячів росії, Білорусі та України. Також можна знайти інформацію щодо PEP-ів з різних країн, охоплення даних по НПД сягає 85 різних міжнародних джерел. Також система показує бізнес-зв'язки таких осіб, в тому числі і історичні також, їх сімейні та особисті зв'язки. Розглянемо це на прикладі голови уряду російської федерації (*рис. 21*).

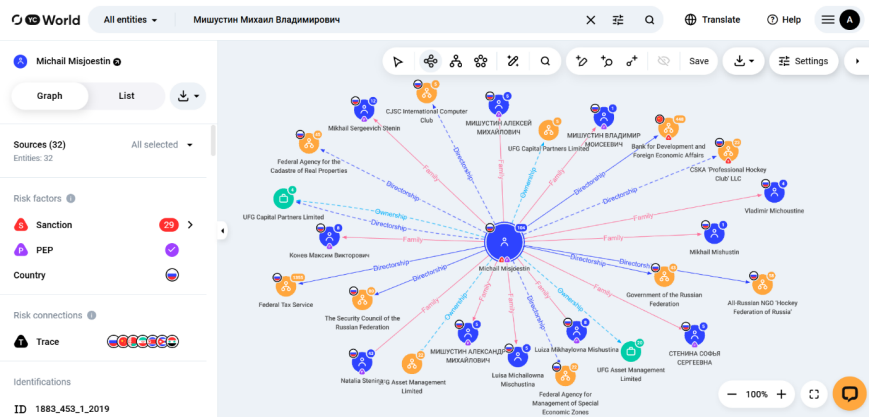

Рисунок 21. Візуалізація зв'язків національних публічних діячів

ВИСНОВОК

Розробка національних інструментів для OSINT-аналізу є важливим етапом у формуванні технологічної спроможності України в умовах гібридних загроз та інформаційної турбулентності. Представлений підхід демонструє здатність поєднувати автоматизований збір даних із глибокою структурною обробкою, що дозволяє ефективно працювати з великими масивами відкритої інформації.

Особливу цінність становить орієнтація на:

– *масштабованість і гнучкість*, що забезпечує адаптацію до різних сценаріїв – від моніторингу до розслідувань;

– *інтеграцію з аналітичними моделями*, які дозволяють виявляти закономірності, зв'язки та ризики в багатоканальному середовищі;
– *підтримку етичних стандартів*, включно з прозорістю джерел, верифікацією даних і пояснюваністю результатів;
– *можливість локалізації*, що враховує мовні, правові та культурні особливості українського контексту.

У результаті, подібні рішення не лише підвищують ефективність OSINT-процесів, а й сприяють формуванню нової аналітичної культури – такої, що поєднує технологічну точність із гуманітарною чутливістю, оперативну дієвість із стратегічною глибиною. Це важливий крок до створення стійкої, етично вмотивованої та міжнародно сумісної екосистеми відкритої розвідки.

"Коли дані набувають правового голосу, аналітика стає частиною справедливості" -
Авторська формула

У цій частині ми переходимо від технічної майстерності до правової відповідальності. OSINT більше не живе лише в оперативному просторі — він входить у зали судів, формує доказову базу, і ставить нові питання про межі юрисдикції, допустимість інформації та етику цифрового сліду.

Як зазначав Луї Брендайс, суддя Верховного суду США:

«Світло найкращий дезінфікуючий засіб, а відкритість — найкраща гарантія справедливості.»

Ця частина — про те, як світло OSINT проникає в найскладніші правові зони, включаючи Deep Web і Dark Web, і як держава має навчитися бачити, аналізувати та діяти відповідально.

Ми запрошуємо читача не просто розуміти, а **переосмислити** роль відкритих джерел у правовій системі. Бо там, де інститути адаптуються до нової реальності, народжується не лише нове право — народжується нова довіра.

ІНСТИТУЦІЙНЕ ВТІЛЕННЯ OSINT: правове, процесуальне, юрисдикційне

ЧАСТИНА IV

РОЗДІЛ 17

ФЕНОМЕН OSINT У НАЦІОНАЛЬНІЙ СУДОВІЙ ПРАКТИЦІ

Дмитро ХУДЕНКО

30 листопада 2022 року Європейський суд з прав людини *(далі - ЄСПЛ)* виніс рішення у міждержавній справі ***«Україна та Нідерланди проти Росії»*** (заяви №№ 8019/16, 43800/14, 28525/20)[1], яким установлено відповідальність Російської Федерації за порушення прав людини в окупованому Криму, на Донбасі та у зв'язку зі збиттям літака рейсу ***«MH17»***. Застосування OSINT-доказів, зокрема матеріалів, підготовлених дослідницькою групою Bellingcat, стало ключовим елементом доказової бази, що підкреслило значення відкритих джерел у міжнародних розслідуваннях. Рішення встановило порушення Європейської конвенції з прав людини та прецедентні стандарти для застосування феномену OSINT у судовій практиці, що може вплинути на методологію розгляду майбутніх справ.

В українській судовій практиці одним із перших випадків застосування OSINT-доказів став вирок Солом'янського районного суду міста Києва від 21 листопада 2025 року у справі про державну зраду[2]. У ході розгляду кримінального провадження сторона захисту стверджувала, що орган досудового розслідування застосував інструменти OSINT для аналізу Telegram-акаунтів, що, на їхню думку, призвело до отримання недостовірних відомостей, які лягли в основу обвинувачення. Згідно з матеріалами справи, обвинувачений у період з 1 листопада 2022 року по 26 січня 2023 року, перебуваючи в м. Слов'янську Краматорського району Донецької області в умовах воєнного стану, умисно передавав представникам Російської Федерації через месенджер Telegram відомості про дислокацію підрозділів Збройних Сил України, їхню військову техніку, кількісний і якісний склад, завдаючи шкоди суверенітету, територіальній цілісності, обороноздатності та інформаційній безпеці України.

Суд відхилив доводи захисту, зазначивши, що інструменти OSINT є загальнодоступними і можуть використовуватись в різних сферах для аналізу інформації. Дані, отримані за допомогою OSINT, не мають самостійного доказового значення, а оцінюються в сукупності з іншими доказами, зокрема показами свідків і підтвердженням використання обвинуваченим Telegram-акаунту. Це рішення стало важливим етапом у формуванні стандартів застосування OSINT-доказів у національній судовій практиці, підтверджуючи їхню легітимність як допоміжного інструменту досудового розслідування за умови комплексної оцінки доказів.

Обидві позиції суду ми поділяємо тому, що вони не суперечать Основному закону, зокрема, положенням статей 17, 31 та 32. Проте навіть така можливість означає дотримання норм міжнародного гуманітарного права та законів війни.

Використання OSINT у судовій практиці зумовлене необхідністю ефективної протидії збройній агресії Російської Федерації та злочинності в умовах четвертої промислової революції. У кримінальному судочинстві поява OSINT-доказів обумовлена обмеженою ефективністю традиційних методів, таких як міжнародна правова допомога, особливо в умовах воєнного стану. OSINT забезпечує оперативний доступ до інформації з відкритих джерел, що не вимагає міжнародних угод і дозволяє компенсувати недоліки традиційних підходів.

[1] Decision ECHR 30.11.2022 CASE OF UKRAINE AND THE NETHERLANDS v. RUSSIA (Applications nos. 8019/16, 43800/14 and 28525/20) URL: https://hudoc.echr.coe.int/eng?i=001-222889.

[2] Вирок Солом›янського районного суду міста Києва від 21.02.2025 у судовій справі № 1-кп/760/1915/25. URL: https://reyestr.court.gov.ua/Review/125919734.

Особливістю OSINT є його доступність і здатність отримувати множинні дані з одного джерела, що робить його інноваційним інструментом для розслідувань. У сучасних умовах, коли цифрові сліди зростають, а традиційні методи збору доказів ускладнені через закриті кордони чи швидке зникнення інформації, комбінація традиційних та інноваційних підходів стає необхідною. Використання OSINT характеризується такими ознаками технологічної революції: автоматизація пошуку та аналізу даних і інформації; інноваційність, яка відкрила нові можливості для здобуття даних чи інформації, їх перевірки; інтеграція засобів і методів у комплексні системи роботи з даними та інформацією; адаптація до цифрових джерел інформації; трансформація існуючих та поширених підходів у досудовому розслідувані, оперативно-розшукової діяльності та кримінальному аналізу.

У нашому випадку судові рішення, зокрема вироки, є юридичним відображенням ефективності застосування OSINT. Для аналізу цього феномену та його сприйняття правоохоронними органами, судами, адвокатурою та іншими учасниками судового процесу досліджено записи Єдиного державного реєстру судових рішень *(далі – ЄРСР)*[3].

ОПИС ДОСЛІДЖЕННЯ

Вибірку судових рішень здійснено шляхом формування пошукових запитів до ЄРСР за ключовими словосполученнями: *«розвідка з відкритих джерел»*, *«open source intelligence»*, *«open-source intelligence»* та абревіатурою *«OSINT»*. Станом на 25 червня 2025 року позитивний результат отримано лише за запитом *«OSINT»*, який охопив період 2019–2025 років. За даними реєстру, повернуто 161 судове рішення першої та апеляційної інстанцій.

Контент-аналіз показав, що у 161 рішенні зафіксовано 205 згадувань OSINT, які стосуються 98 судових справ та 67 кримінальних проваджень, зокрема двох іноземних.

Варто зазначити, що у деяких судових рішеннях назви актів були помилковими або визнаними нерепрезентативними. Наприклад, у таблиці результатів пошуку в ЄРСР зазначено більшу кількість вироків, ніж фактично виявлено, оскільки окремі рішення, позначені як вироки, за змістом були ухвалами, зокрема, ухвала Центрального районного суду м. Миколаєва від 05 серпня 2022 року у судовій справі № 490/2946/22[4].

Рішення апеляційної інстанції (7 рішень, або 4,3 %, з 11 згадуваннями у 7 справах і 4 провадженнях) не враховано через їхню незначну кількість та ризик дублювання даних із першою інстанцією. Крім того, аналіз обмежено публічним сегментом ЄРСР, що не повною мірою відображає стан справ, але дозволяє зробити репрезентативні висновки. До того ж, за період написання даного матеріалу було оприлюднено ще 5 судових рішень, що ймовірно стануть предметом майбутніх наукових розвідок.

Для подальшого дослідження визнано доцільними 154 судові рішення першої інстанції, які містять 194 згадування OSINT у 92 справах і 63 кримінальних провадженнях. Частота згадувань на одне рішення становить 1,3 раза, при цьому 40 рішень (26 %) містять від 2 до 5 згадувань, що становить 94 згадування (48,5 %) у 21 справі (22,8 %).

Феномен OSINT проявляється як у досудовому розслідуванні та оперативно-розшуковій діяльності, так і в контексті злочинної діяльності. У першому випадку OSINT має суспільно корисне значення за умови дотримання правових норм, тоді як у другому – спричиняє суспільну шкоду.

[3] Єдиний реєстр судових рішень. URL: https://reyestr.court.gov.ua.

[4] Ухвала Центрального районного суду м. Миколаєва від 08.08.2022 у судовій справі № 1-кп/490/446/2022. URL: https://reyestr.court.gov.ua/Review/106005639.

аналіз соціальних мереж, технічних ідентифікаторів, діяльності юридичних осіб, функцій військових підрозділів, фіксацію доказів і надання експертної підтримки. Юридичні підстави, які регламентовано статтями 40–41, 71, 93, 224, 237, 545–552 КПК України та форми фіксації (протоколи, рапорти) забезпечують його правову основу.

Хронологічний і регіональний розподіл рішень відображає зростання ролі OSINT після 2022 року через воєнний стан. Участь правоохоронних органів, серед яких СБУ, НПУ та БЕБ, громадських організацій – Molfar та Global Rights Compliance, а також незалежних фахівців підкреслює його демократизацію.

Суди визнають OSINT-докази допустимими в комплексі з іншими доказами за умови відповідності стандартам ЄСПЛ, а також вимогам *«Протоколу Берклі»* щодо збору, перевірки та фіксації даних. Це забезпечує баланс між ефективністю розслідувань і захистом прав людини.

OSINT як феномен потребує подальшого правового регулювання, зокрема чіткого визначення процедур фіксації доказів і меж використання, щоб уникнути зловживань і забезпечити єдність судової практики. Розвиток цифрових технологій і зростання обсягу відкритих даних роблять OSINT незамінним інструментом у протидії сучасним викликам, зокрема кіберзлочинності, шахрайству та гібридній війні.

РОЗДІЛ 18

ЕЛЕКТРОННІ ДОКАЗИ В КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПРОБЛЕМИ ЗБИРАННЯ ТА ВИКОРИСТАННЯ В ДОКАЗУВАННІ

Людмила ГАВРИЛЮК

В умовах стрімкого розвитку інформаційних технологій, взаємодія із цифровим світом є частиною повсякденного життя кожної людини. Інформація в електронній (цифровій) формі може відображати відомості про присутність певної особи або про її діяльність у цифровому просторі у певний відрізок часу, різні фото, відеозаписи, повідомлення, документи, тощо. Досить часто інформація в електронній (цифровій) формі із різних джерел може містити фактичні дані на підставі яких слідчий, прокурор, слідчий суддя і суд можуть встановити наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. Така інформація може бути як допоміжним, так і основним або єдиним інструментом встановлення всіх обставин справи.

На сьогодні *інформація в електронній (цифровій) формі*, що містить дані про обставини, які мають значення для справи, зокрема електронні документи (у тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі і можуть зберігатися на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, в інших місцях зберігання даних в електронній формі (у тому числі в мережі *«Інтернет»* у Цивільному процесуальному кодексі України (ЦПК) (ч. 1 ст. 100)[1], Господарському

[1] Цивільний процесуальний кодекс України: Закон України від 18.03.2004 р. № 1618-IV. Відомості Верховної Ради України. 2004. № 40–41, 42. Ст. 492. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text.

процесуальному кодексі України (ГПК) (ч. 1 ст. 96)[2] та у Кодексі адміністративного судочинства України (КАС) (ч. 1 ст. 99)[3] *визначається як* **електронні докази**.

В КПК визначення терміну *«електронні докази»* не унормовано, а зазначенні у ч. 2 ст. 84 КПК джерела доказів не дають можливості розглядати електронні докази як окреме процесуальне джерело доказів, ознаки якого простежуються у його нормах, які регулюють доказування у кримінальному провадженні.

Так, згідно з ч. 2 ст. 84 КПК процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів. Відповідно до ч. 1 ст. 99 КПК *документом* є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, що можуть бути використані як доказ факту чи обставин, які встановлюються під час кримінального провадження[4]. Такі носії інформації, як матеріали фотозйомки, звукозапису, відеозапису, інші носії інформації, у тому числі комп'ютерні дані, також віднесені до категорії *«документ»* (ч. 2 ст. 99 КПК). Отже, до категорії *«електронні докази»* у кримінальному процесі України за аналогією із наведеним визначенням цього терміну у ЦПК, ГПК та КАС віднесена інформацію в електронній (цифровій) формі, що зафіксована:

1. *в електронному документі;*
2. *у матеріалах фотозйомки;*
3. *у матеріалах звукозапису;*
4. *у матеріалах відеозапису;*
5. *на інших носіях інформації (у тому числі комп'ютерні дані).*

Водночас, згідно з ч. 2 ст. 98 КПК документ може бути і речовим доказом, якщо він був знаряддям вчинення кримінального правопорушення, зберіг на собі його сліди або містить інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження.

Отже, *електронний доказ в кримінальному провадженні* слід розглядати як інформацію в електронній (цифровій) формі, що отримана в передбаченому КПК порядку і має значення для кримінального провадження.

Одним із видів документа як процесуального джерела доказу (ст. 99 КПК) є **електронний документ**, який може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму. Стаття 6 Закону України *«Про електронні документи та електронний документообіг»* передбачає, що для ідентифікації автора електронного документа може бути використаний електронний підпис, а для підтвердження достовірності походження та цілісності електронного документа може використовуватися електронна печатка[5]. Особливістю електронного документу є те, що у ньому інформація зафіксована у вигляді *електронних даних*, включаючи обов'язкові реквізити документа[6]. Склад і порядок розміщення обов'язкових реквізитів електронних документів визначаються законодавством.

Згідно з ч. 1, абз. 2 ч. 2 ст. 237 КПК, електронний документ *набуває процесуального значення доказу після його огляду*, за умови виявлення слідчим, прокурором, під час такого огляду відомостей щодо обставин вчинення кримінального правопорушення, які мають бути належним чином зафіксовані у протоколі огляду.

---

[2] Господарський процесуальний кодекс України: Закон України від 06.11.1991 р. № 1798-XII. Відомості Верховної Ради України. 1992. № 6. Ст. 56. URL: https://zakon.rada.gov.ua/laws/show/1798-12#Text.

[3] Кодекс адміністративного судочинства України: Закон України від 06.07.2005 р. № 2747-IV. Відомості Верховної Ради України. 2005. № 35–36, 37. Ст. 446. URL: https://zakon.rada.gov.ua/laws/show/2747-15#Text.

[4] Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651–VI: станом на 19.04.2024 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17.

[5] Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. Відомості Верховної Ради України. 2003. № 36. Ст. 275. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

[6] Там само.

провадження. *Наприклад*. Якщо електронний доказ утворився у зв'язку з конкретними діями підозрюваної особи, то слідчий має встановити і зафіксувати процес, спосіб їх створення, визначити електронний пристрій, за допомогою якого це було вчинено, та встановити усіх осіб, причетних до протиправних дій.

Якщо слідчий досліджує електронний доказ, до створення якого непричетна підозрювана особа, але на ньому зафіксовано її протиправні дії, то методи, цілі, способи збирання і дослідження такої інформації будуть різнитися від попередньої ситуації. У такому випадку слідчий буде досліджувати зафіксовану інформацію, яка буде підтверджувати чи спростовувати якісь факти у сукупності з іншими доказами щодо вчиненого кримінального правопорушення, а також спосіб її походження.

Такими носіями інформації можуть бути:

- подані потерпілим, підозрюваним, свідком, іншими учасниками кримінального провадження фото, відеозаписи, скріншоти фото, окремих кадрів відеозаписів, фрагменти контенту вебсайтів, сторінок у соціальних мережах тощо;
- отриманні слідчим у результаті проведення слідчих (розшукових), негласних слідчих (розшукових) та інших процесуальних дій;
- отримані слідчим у результаті фіксування процесуальної дії за допомогою технічних засобів фіксації кримінального провадження відповідно до вимог ст. 107 КПК;
- ті, які надійшли з матеріалами, в яких зафіксовано фактичні дані про протиправні діяння окремих осіб і груп осіб, які зібрані оперативними підрозділами з дотриманням вимог Закону України *«Про оперативно-розшукову діяльність»* тощо.

Оцінювання інформації в електронній (цифровій) формі, яку слідчому необхідно буде зібрати, дає можливість визначити методику роботи з нею. З точки зору невідкладності, визначаючи спосіб і які докази слід отримати першочергово, треба керуватися наявною інформацією про ймовірність приховування, знищення, зміну інформації в електронній (цифровій) формі, яка містить фактичні дані, що мають значення для кримінального провадження і підлягають доказуванню. Розглянемо деякі типові слідчі ситуації, які найчастіше трапляються на практиці.

Згідно вимог КПК щодо критеріїв допустимості доказів кожний доказ має відповідати певним вимогам. Окрім, під час збирання такої інформації в кримінальному провадженні слід керуватися ст.ст. 84-86 КПК, а саме *інформація в електронній (цифровій) формі набуде статусу доказу, якщо:*

1. *прямо чи непрямо підтверджує існування чи відсутність обставин, що підлягають доказуванню у кримінальному провадженні, та інших обставин, які мають значення для кримінального провадження, а також достовірність чи недостовірність, можливість чи неможливість використання інших доказів;*
2. *отримана у порядку, встановленому КПК.*

Водночас, електронний доказ має *відповідати загальним критеріям допустимості доказів* відповідно до КПК й має бути отриманий:

1. належним суб'єктом;
2. із дотримання процесуальної форми збирання та фіксації;
3. з належного процесуального джерела.

У випадку порушення цих вимог, електронний доказ може бути визнаний недопустимий, у зв'язку з чим не може бути використаний під час прийняття процесуальних рішень, на нього не може посилатися суд під час ухвалення судового рішення.

РОЗДІЛ 19

ТЕРИТОРІАЛЬНА ЮРИСДИКЦІЯ OSINT

Дмитро ХУДЕНКО

Нормами права прямої дії встановлено режим здійснення державної влади та правовий порядок на всій території Україні (ст. 2, ч. 2 ст. 6, ч. 2 ст. 19 [1]).

Територіальні межі досудового розслідування, оперативно-розшукової діяльності та кримінального аналізу, у яких останнім часом активно використовують відкриті джерела, охоплено окремою правовою дефініцією – територіальна юрисдикція. Дотримання меж сприяє нівелюванню дублювання між органами та службами в структурі органу державної виконавчої влади та між ними. Чітка правова регламентація територіальної юрисдикції виступає гарантіями захисту прав осіб, а також основ забезпечення правопорядку та законності під час розслідування кримінальних правопорушень, розшуку обвинувачених, підсудних, осіб, які ухиляються від відбування кримінального покарання, безвісно зниклих осіб та встановлення особи невпізнаних трупів.

Для забезпечення невідворотності юридичної відповідальності, особливо коли підозрювані або обвинувачені у кримінальних правопорушень проти миру, безпеки людства та міжнародного правопорядку знаходяться за межами України, допускається процедура in absentia, що у перекладі з латинської мови означає – у відсутності. Протягом попередніх трьох років поширено винесення судових рішень за цією процедурою через різке погіршення криміногенного стану, що у свою чергу обумовлено новою хвилею військової агресії рф проти України. За нашими підрахунками Єдиний реєстр судових рішень містив до 24 лютого 2022 р. 406 ухвалених рішень з кримінального судочинства, у яких згадано in absentia та кваліфікацію за ст. 438 КК України *«Воєнні злочини»*. Станом на 19 серпня 2025 р. додано ще 6042 таких судових рішень[2].

Водночас, опитування представників органів прокуратури України щодо складнощів розслідування об'єктивно показало відсутність доступу до місця злочину на окупованій території, складність отримання доказів, зокрема через те, що більшість свідків перебувають на таких територіях тощо[3].

У протидії воєнним злочинам використання феномену OSINT є однією з останніх та найдинамічніших тенденцій, який довів ефективність. Завдяки йому стало за можливе відпрацювати обставини різнорідних складів кримінальних правопорушень, встановити, розпізнати та ідентифікувати потенційних підозрюваних, відстежити ворожу активність та логістику, а також з'ясувати місцезнаходження протиправно набутих активів або речей чи культурних цінностей, які незаконно переміщено за кордон.

Вищенаведені факти дозволяють перейти до складових наукової проблематики у галузі кримінального процесу, оперативно-розшукової діяльності та

[1] Конституція України від 28.06.1996. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text. – Назва з екрана. – Дата звернення: 02.02.2025.

[2] Єдиний державний реєстр судових рішень [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/. – Назва з екрана. – Дата звернення: 19.08.2025.

[3] Міжнародні злочини в Україні: огляд національного розслідування та судової практики. 2023. С.47-48. [Електронний ресурс]. — Режим доступу: https://www.helsinki.org.ua/wpcontent/uploads/2023/09/International_crim_ukr_A4-DLYA-ONLAYN-PUBLIKATSIYI-3.pdf. – Назва з екрана. – Дата звернення: 03.08.2025.

кримінального аналізу, які потребують розв'язання, стосуються теорії і практики, нових знань, викликів та реалій.

По-перше, існує суперечність між формальним поширенням юрисдикції на всю територію України та об'єктивною неможливістю реалізації на окупованих територіях повного комплексу слідчих (розшукових) дій та оперативно-розшукових заходів, передбачених чинним законодавством. Майже те ж саме стосується і міжнародних угод про правову допомогу із державою-агресором. Це призводить до парадоксу, за яким по суті де-юре має бути, але де-факто відсутнє, що загострює потребу розробки та впровадження компенсаторних методологій.

По-друге, констатуємо часткову нормативно-правову невизначеність регламентації територіальної юрисдикції OSINT або прогалини в праві, що загострює ризики легітимності збирання доказів, а також доказування.

Поміж багатьох найважливіших завдань, що постають перед Україною і мають негайно вирішуватись, існують мінімум два основні або екзистенційні – захист та оборона України, як держави, а також захист людини, її прав і свобод. Можливо розв'язання складових проблеми безпосередньо не вирішіть усіх завдань, але однозначно буде цьому сприяти.

У юридичній науці розв'язання поставленої проблематики тісно пов'язано з вирішенням актуальних питань кримінального процесу, оперативно-розшукової діяльності та кримінального аналізу, серед яких назвемо потребу подальшої розробки теоретичних основ і особливостей нормативно-правового регулювання юрисдикції, збирання доказів, методик розслідування та розкриття окремих видів кримінальних правопорушень, розшуку безвісно відсутніх осіб за особливих обставин тощо.

Вагоме значення у дослідженні цієї проблематики мають джерела, які стосуються єдиного підходу та рекомендацій щодо відкритих джерел, як-то Протокол з проведення розслідувань із використанням відкритих цифрових даних (Нью-Йорк, Женєва, 2022)[4], Лейденські рекомендації щодо цифрових доказів (Лейден, 2022)[5], Керівництво з базових стандартів розслідування для документування міжнародних злочинів в Україні (Гаага, 2023)[6], Оцінка цифрових зображень з відкритих джерел (Берлін, 2024)[7] тощо.

Фундаментальну цінність несуть сучасні академічні праці, серед яких «Тактичний кримінальний аналіз: теорія та практика (Одеса, 2019)[8], *«Основи кримінального аналізу»* (Львів, 2021)[9], *«Основи кримінального аналізу: теорія та практика застосування в оперативних підрозділах Державної прикордонної служби України»* (Хмельницький, 2022)[10], *«Основи кримінального аналізу»*

[4] Протокол Беркли по ведению расследований с использованием открытых цифровых данных : практическое руководство по эффективному использованию открытых цифровых данных [Електронний ресурс] / Організація Об'єднаних Націй, Управління Верховного комісара з прав людини ; Центр з прав людини при Школі права Каліфорнійського університету в Берклі. – Нью-Йорк ; Женева : ООН, 2022. – 87 с. – Режим доступу: https://www.ohchr.org/sites/default/files/2022-12/Berkeley-Protocol-Russian.pdf. – Назва з екрана. – Дата звернення: 10.08.2025.

[5] Leiden Guidelines on the Use of Digitally Derived Evidence in International Criminal Courts and Tribunals [Електронний ресурс] / Sofia Aalto-Setälä, Luca Caroli, Sabrina K. Rewald, Julia Freytag, Maria F. Jaramillo Gomez ; coord. Joshua Lim, Robert Heinsch. – Leiden : Kalshoven-Gieskes Forum on International Humanitarian Law, 2022. – 54 с. – Режим доступу: https://leiden-guidelines.com/assets/Leiden%20Guidelines%20on%20the%20Use%20of%20DDE%20in%20ICCTs_20220404.pdf. – Назва з екрана. – Дата звернення: 19.07.2025.

[6] Керівництво з базових стандартів розслідування для документування міжнародних злочинів в Україні : довідники. – Гаага : Global Rights Compliance, 2023. – 92 с. – Режим доступу: https://www.asser.nl/media/796397/manual-керівництво-з-базових-стандартів-розслідування-для-документування-міжнародних-злочинів-в-укрaі-ні-довідники-1.pdf. – Назва з екрана. – Дата звернення: 01.07.2025.

[7] Оцінка цифрових знімків з відкритих джерел: Посібник для суддів і дослідників фактів [Електронний ресурс] / Башак Чали, Джозеф Фіннерті, Ліндсі Фріман, Алекса Кеніг, Ліббі МакЕвой, Івонн МакДермотт Різ, Дараг Мюррей, Яна Садлер-Форстер, Ракель Васкес Льоренте, Сара Зармські. – 2024. – 37 с. – Режим доступу: https://www.trueproject.co.uk/_files/ugd/55728f_c247e350c0de42e6ad5c39fbf9d5104a.pdf, вільний. – Назва з екрана. – Дата звернення: 10.08.2025.

[8] 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.

[9] Федчак І. А. Основи кримінального аналізу : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2021. - 288 с.

[10] Основи кримінального аналізу: теорія та практика застосування в оперативних підрозділах Державної прикордонної служби України : навчальний посібник / О. С. Кіреєва, Ю. В. Крутік, О. М. Махлай, А. С. Треус. Хмельницький : Вид-во НАДПСУ, 2022. - 360 с

та підтвердженням місця розташування, фіксацією походження й руху доказу, приватністю, універсальною юрисдикцією, поєднанням різних даних та оцінкою ризиків, які розподілено по різних пунктах документу.

Наприклад, вже у вступі до Лейденських рекомендаціях щодо цифрових доказів вказано, що свідчення очевидця може дати корисні відомості про подію, натомість супутникове зображення здатне виявити те, що недосяжно для безпосереднього спостереження.

Посібник *«Оцінка цифрових зображень з відкритих джерел»*[70] створений з метою допомогти суддям, правозахисникам і дослідникам фактів у судових процесах і розслідуваннях порушень прав людини містить декілька згадок про бар'єри доступу до територій та прецеденти універсальної судової юрисдикції.

Наприклад, урядові бар'єри доступу до територій описані щодо районів Гази чи Сіньцзянь. Також присутні згадки про використання цифрових зображень з відкритих джерел у справах Міжнародного кримінального суду та Європейського суду з прав людини.

У Керівництві з базових стандартів розслідування для документування міжнародних злочинів в Україні (Гаага, 2023)[71] містяться роз'яснення окупації, екстериторіальної юрисдикції та ефективного контролю в контексті міжнародного права, зокрема міжнародного права прав людини та міжнародного гуманітарного права. Документ аналізує юрисдикцію держав, зосереджуючись на ефективному контролі над особами чи територіями, та висвітлює відповідальність держави-окупанта, зокрема рф, за дотримання прав людини на окупованих територіях, таких як Крим і окремі райони Донбасу.

Розділ п'ятий стосується збору та збереження інформації. Він починається з ознайомленням з інформацією / доказами та огляду вимог щодо допустимості доказів. В розділі описуються конкретні кроки, які повинні зробити фахівці щодо отримання, запису, обробки, збереження і автентифікації різних категорій інформації, включно з фізичною, цифровою і розвідкою з відкритих джерел на всій території України.

ПРАКТИКА ЗАСТОСУВАННЯ ТЕРИТОРІАЛЬНОЇ ЮРИСДИКЦІЇ У КРИМІНАЛЬНОМУ АНАЛІЗІ БЕЗПЕКИ ДЕРЖАВНОГО КОРДОНУ

У сфері прикордонної безпеки існує практика, згідно з якою для цілей кримінального аналізу та оцінки загроз можуть використовуватись дані, отримані з джерел[72], що фізично перебувають поза межами України, зокрема з іноземних державних реєстрів.

Залежно від рівня аналізу ризиків у ДПСУ з використанням спільної інтегрованої моделі аналізу ризиків держав - членів ЄС визнано за можливе встановлення різновидів глобальних загроз, під якими розуміють загальнодержавні загрози, дія яких поширюється за межі України.

За результатами оцінки загроз визначаються зовнішні та внутрішні фактори, які негативно впливають (діють) на сферу безпеки державного кордону. Визначення таких факторів впливу здійснюється з урахуванням чотирирівневої системи контролю за в'їздом та перебуванням в Україні іноземців та осіб без громадянства, два рівні якої перебувають у країнах походження незаконних

[70] Оцінка цифрових знімків з відкритих джерел: Посібник для суддів і дослідників фактів [Електронний ресурс] / Башак Чали, Джозеф Фіннерті, Ліндсі Фріман, Алекса Кеніг, Ліббі МакЕвой, Івонн МакДермотт Різ, Дараг Мюррей, Яна Садлер-Форстер, Ракель Васкес Льоренте, Сара Зармські. – 2024. – 37 с. – Режим доступу: https://www.trueproject.co.uk/_files/ugd/55728f_c247e350c0de42e6ad5c39fbf9d5104a.pdf, вільний. – Назва з екрана. – Дата звернення: 10.08.2025.

[71] Керівництво з базових стандартів розслідування для документування міжнародних злочинів в Україні : довідники. – Гаага : Global Rights Compliance, 2023. – 552 с. – Режим доступу: https://globalrightscompliance.org/wp-content/uploads/2025/06/КЕРІВНИЦТВО-З-БАЗОВИХ-СТАНДАРТІВ-РОЗСЛІДУВАННЯ-ДЛЯ-ДОКУМЕНТУВАННЯ-МІЖНАРОДНИХ-ЗЛОЧИНІВ-В-УКРАЇНІ.pdf. – Назва з екрана. – Дата звернення: 01.07.2025.

[72] Основи кримінального аналізу: теорія та практика застосування в оперативних підрозділах Державної прикордонної служби України : навчальний посібник / О. С. Кіреєва, Ю. В. Крутік, О. М. Махлай, А. С. Треус. Хмельницький : Вид-во НАДПСУ, 2022. - 360 с. – С. 339.

мігрантів або у державах, що межують з Україною[73].

Такий підхід відповідає інтегрованій моделі оцінки ризиків країн ЄС, де нормативно визнано, що загрози можуть мати глобальний характер та діяти поза межами національного суверенітету, а відповідно й впливати на внутрішню безпеку України, зокрема, на охорону державного кордону.

Розглянута суть практики свідчить про функціональне розширення поняття юрисдикції не лише в межах територіальних меж, а й у контексті попереджувального контролю та кримінального аналізу, якими охоплено фактори іноземного походження, зокрема на територіях країн ризику або суміжних держав.

ВИСНОВОК

Узагальнюючи результати дослідження, слід констатувати, що правове регулювання територіальної юрисдикції в OSINT-діяльності перебуває на етапі формування та потребує концептуального уточнення. Відсутність законодавчої дефініції OSINT зумовлює необхідність уніфікації понятійно-категоріального апарату, а суперечність між формальним поширенням юрисдикції України та фактичною неможливістю її реалізації на окупованих територіях чи у кіберпросторі актуалізує потребу у компенсаторних методологіях. Запропоноване розмежування транскордонної та зовнішньої методології OSINT створює підґрунтя для легітимного документування злочинів попри юрисдикційні бар'єри. Доказове значення цифрових відомостей з відкритих джерел дедалі частіше визначається не місцем розташування серверів, а принципом наслідків, що узгоджується з міжнародною практикою. Адаптація міжнародних стандартів до українських реалій є важливою умовою формування сучасної системи використання цифрових доказів. Інтеграція OSINT у правоохоронну діяльність сприяє підвищенню ефективності захисту прав людини та забезпечує невідворотність юридичної відповідальності за міжнародні злочини.

РОЗДІЛ 20

ПРАВОВІ АСПЕКТИ ВИКОРИСТАННЯ ДАНИХ ОТРИМАНИХ З DEEP WEB ТА DARK WEB У OSINT-ДОСЛІДЖЕННЯХ, В ЯКОСТІ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ

Дмитро АФОНІН

Сучасний цифровий простір став незамінним джерелом інформації для кримінальних розслідувань, при цьому зростає увага до менш доступних шарів Інтернету. Розвідка на основі відкритих джерел (OSINT) визначається як практика збору та аналізу інформації з публічно доступних джерел для задоволення конкретних розвідувальних потреб. Це охоплює не тільки легко індексований *«Поверхневий веб»* (Surface Web), але й величезний *«Глибинний веб»* (Deep Web) та навмисно прихований *«Темний веб»* (Dark Web).

Хоча Deep Web та Dark Web використовуються в межах правового поля, їхня анонімність та відсутність традиційного контролю зробили їх благодатним ґрунтом для незаконної діяльності, включаючи нелегальний продаж вогнепальної зброї, торгівлю наркотичними засобами та дитячу порнографію.

[73] Про затвердження Інструкції з проведення аналізу ризиків у Державній прикордонній службі України : Наказ МВС України від 11.12.2017 № 1007 [Електронний ресурс]. — Режим доступу: https://zakon.rada.gov.ua/go/z0091-18. — Назва з екрана. — Дата звернення: 03.04.2025.

Виклик для правоохоронних органів полягає в ефективному використанні інформації з цих прихованих областей Інтернету для збору розвідувальних даних (OSINT), забезпечуючи при цьому її *правову допустимість* та подальше використання як *електронних доказів* у кримінальних провадженнях. Але на теперішній час існує багато правових проблем у допустимості визначення даних, отриманих з Deep Web та Dark Web, в якості електронних *«цифрових»* доказів.

> *Чи можна вважати джерела, що знаходяться в Deep Web та Dark Web, «відкритими» та надати всебічний правовий аналіз допустимості визначення даних отриманих із джерел Deep Web та Dark Web для OSINT-досліджень в Україні, як електронних (цифрових) доказів у кримінальних провадженнях?*

Deep Web переважно використовується в правовому полі, в якому розміщуються величезні обсяги академічних, урядових та корпоративних даних, які не індексуються комерційними пошуковими системами. Dark Web також має правові підстави використання, а саме забезпечення безпеки приватного спілкування осіб. Однак анонімність, яка надається в Dark Web, створює підґрунтя саме для злочинної діяльності. До неї відноситься і торгівля наркотиками, нелегальний продаж зброї, торгівля викраденими даними (наприклад, крадіжка особистих даних, дані кредитних карток), відмивання грошей та розповсюдження дитячої порнографії, тероризм, екстремізм тощо[1].

При цьому ключове питання полягає в тому, чи можна вважати джерела, що знаходяться в Deep Web та Dark Web, *«відкритими»* або *«публічно доступними»*.

Існує дві точки зору, щодо цього питання.

Перша, що джерела Deep Web та Dark Web не відносяться до OSINT, у зв'язку з тим, що OSINT базується виключно на легально доступних даних, виключаючи необхідність несанкціонованого доступу або інвазивних (проникаючих, які обходять захист) методів, підкреслюючи головний принцип OSINT – *легальність* та *відкритість*. Так, вхід до Dark Web не є злочином у багатьох країнах, але взаємодія з великою частиною його контенту (торгівля наркотиками, зброєю, викраденими даними) є протиправною. Також використання Tor та інших засобів анонімізації вже виходить за межі простого *«публічного доступу»*.

Друга, – джерела Deep Web та Dark Web відносяться до OSINT. Це аргументується тим, що технічний доступ до нього є безкоштовним і він не має єдиного власника[2].

Ця розбіжність у поглядах підкреслює фундаментальну напругу.

Якщо *«публічно доступний»* означає легкий доступ без аутентифікації чи спеціальних інструментів, то Deep Web (який часто вимагає облікових даних) та Dark Web (який вимагає спеціалізованих браузерів, таких як Tor) *не відповідають цьому критерію*.

Проте, якщо *«публічно доступний»* інтерпретується як інформація, яка не є приватною за своєю природою (наприклад, не захищена паролем або не є частиною закритої системи), або інформація, яка, хоч і прихована, але може бути отримана без злому чи несанкціонованого обходу систем безпеки, то тоді Deep та Dark Web *можуть містити «відкриті» джерела*.

Важливою відмінністю є те, що OSINT не повинен бути схожий на хакерство або несанкціонований доступ до даних[3].

---

[1] Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі) : наук.-практ. порадник / Л.В. Гаврилюк, І.В. Басиста, Д.С. Афонін, А.В. Шевчишен та ін. ; за заг. ред. М.С. Цуцкіридзе. – Київ : ДНДІ МВС України; Вид-во «Політехніка», 2024. 196 с.

[2] Dark Web vs Deep Web OSINT Investigations. Blackdot Solutions. URL: https://blackdotsolutions.com/blog/dark-web-vs-deep-web/ (дата звернення: 10.06.2025).

[3] Використання методології OSINT для отримання оперативно-значимої інформації : методичні рекомендації / Д.С. Афонін, Д.В. Лісніченко, О.М. Заєць. Одеса, ОДУВС, 2024. 39 с.

Заохочення залучення експертних висновків від сертифікованих фахівців з цифрової криміналістики на ранніх стадіях розслідування є ключовим для підвищення доказової цінності.

7. *Забезпечення балансу між ефективністю розслідувань та захистом прав людини*. Будь-які слідчі (розшукові) дії, особливо ті, що стосуються Deep Web/Dark Web, повинні суворо дотримуватися стандартів прав людини та конституційних прав. Необхідно впровадити надійні гарантії захисту персональних даних під час збору доказів OSINT інструментами та методами. Важливо сприяти прозорості та підзвітності у використанні передових методів розслідування.

ВИСНОВОК

Використання джерел з Deep Web та Dark Web для OSINT-досліджень та як електронних доказів у кримінальних провадженнях в Україні є складною та багатогранною проблемою, що вимагає негайного вирішення. Хоча OSINT визнається цінним інструментом для збору розвідувальних даних, особливо з Deep Web, його застосування до Dark Web та подальша допустимість отриманих даних як доказів стикаються зі значними правовими та технічними перешкодами.

Ключова відмінність між Deep Web та Dark Web, що базується на намірі приховування, має вирішальне значення для визначення правових рамок доступу. Українське законодавство, зокрема КПК України, наразі не містить чіткого визначення *«електронних доказів»*, трактуючи їх як *«документи»*, що створює концептуальні та практичні складнощі. Вимоги до оригінальності, метаданих та ланцюга безперервності для електронних доказів є суворими, а їх недотримання може призвести до недопустимості. Існуючі процесуальні інструменти, такі як тимчасовий доступ та обшук, часто виявляються недостатніми для роботи з анонімними та розподіленими даними Deep Web та Dark Web. Хоча негласні слідчі (розшукові) дії, зокрема зняття інформації з електронних інформаційних систем (ст. 264 КПК), охоплюють OSINT, це створює напругу між *«відкритим»* характером OSINT та вимогами до *«негласних»* дій.

Особливі виклики, такі як анонімність, волатильність, проблеми цілісності та автентичності, а також транскордонний характер злочинів, ускладнюють доказування злочинів, пов'язаних з незаконним продажем зброї, наркотиків та порнографії. Судова практика України, хоча й визнає електронні докази, потребує більш конкретних прецедентів щодо даних з Deep Web та Dark Web. Існуючі правові прогалини та *«регуляторне відставання»* створюють правову невизначеність та перешкоджають ефективному судовому переслідуванню. Додатковим критичним аспектом є ризик деанонімізації слідчих та необхідність захисту персональних даних, що вимагає балансу між ефективністю розслідувань та дотриманням прав людини.

Для подолання цих викликів необхідний комплексний підхід, що включає:

1. *Законодавчі реформи*: Чітке визначення електронних доказів та OSINT у КПК України, розробка спеціальних положень для даних з Deep Web/Dark Web та регулювання спеціалізованих методів розслідування, а також оновлення законодавства про захист даних.
2. *Посилення міжнародного співробітництва*: Повна імплементація Другого Додаткового Протоколу до Будапештської конвенції та зміцнення партнерств з технологічними компаніями.
3. *Розвиток цифрової криміналістики*: Інвестиції у можливості цифрової криміналістики, безперервне навчання для правоохоронних органів та судових працівників.
4. *Розробка чітких протоколів*: Впровадження стандартизованих процедур

для збору, збереження та аналізу доказів з Deep Web/Dark Web, з акцентом на метаданих та ланцюгу безперервності.

5. *Забезпечення прав людини*: Завжди дотримуватися стандартів прав людини та конституційних прав під час усіх слідчих дій.

Вирішення цих правових прогалин та практичних проблем є першочерговим завданням для України, щоб забезпечити ефективне правосуддя в цифрову епоху та посилити боротьбу з кіберзлочинністю, що походить з прихованих шарів інтернету.

Наукове видання

OSINT OPEN SOURCE INTELLIGENCE
ТЕОРІЯ ТА МЕТОДОЛОГІЯ

МОНОГРАФІЯ

Користін О., Демедюк С., Барановський О., Ланде Д. та ін.,
за заг. ред. Користіна О.Є., Демедюка С.В.

Комп'ютерна верстка: Федчук Сергій

Підписано до друку 18.11.2025. Формат 70х100/16
Папір крейдовий. Друк цифровий.
Ум. друк. арк. 9,5. Зам. № 1811-25/3.
Наклад 100 прим.

Видавець і виготовлювач ТОВ «7БЦ»
03067, м. Київ, вул. Олекси Тихого, 84
e-mail: 7bc@ukr.net, тел: (044) 592-00-80
Свідоцтво суб'єкта видавничої справи ДК №5329 від 11.04.2017