Олександр КОРИСТІН Сергій ДЕМЕДЮК

OSINT

OPEN SOURCE INTELLIGENCE

КНИГА 2

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

Олександр КОРИСТІН Сергій ДЕМЕДЮК

OSINT
OPEN SOURCE INTELLIGENCE

Інструменти та методи

Видано за підтримки
CRDF Global в Україні

CRDF GLOBAL

2025

УДК 004.056.5:351.861:351.746.1(075)

О 73

DOI: 10.32782/osint-instruments-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. Інструменти та методи: навчальний посібник / Користін О., Демедюк С., Ісмайлов К., Ланде Д. та ін., за заг. ред. Користіна О.Є., Демедюка С.В. – Київ: 7БЦ, 2025. 460 с.
ISBN 978-617-8794-17-0

Навчальний посібник "OSINT: інструменти та методи" є прикладним продовженням монографії й орієнтований на формування практичних компетентностей аналітика відкритих джерел. Посібник починається з безпеки процесу: операційна безпека, анонімність, налаштування робочого середовища для OSINT-операцій (VPN, менеджери паролів, віртуальні машини, веббраузери) та протидія кіберризикам.

Далі подано систематизований огляд інструментарію: фреймворки, пошукові системи, соціальні мережі, вебархіви, WHOIS, державні реєстри, віртуальні валюти, метадані, аналіз фото й відео та розпізнавання обличь, мобільні застосунки і телеграм-боти, технології ШІ для збору даних, середовища Python, візуалізація та Maltego. Окремий розділ присвячено практичному застосуванню ШІ та Python: промпт-інженерія без коду, кейси кібербезпеки й інцидент-респонсу, моніторинг гібридних загроз і дезінформації, пошук зниклих осіб і документування порушень прав людини; інструменти big data, базові функції OSINT-скриптів і приклади фінансової аналітики за медійним слідом.

Завершальні частини фокусуються на цільових ресурсах документування воєнних злочинів і процесуальних механізмах збирання електронних доказів,.

Посібник адресовано практикам сектору безпеки й оборони, правоохоронцям, юристам, журналістам-розслідувачам, аналітикам, викладачам і студентам – усім, хто вибудовує професійну, етичну та технологічно зрілу OSINT-екосистему України.

УДК 004.056.5:351.861:351.746.1(075)

ISBN 978-617-8794-17-0

Ця праця — для тих, хто зводить мости між видимим і прихованим, перетворюючи крихти фактів на щити правди та мечі справедливості.

Для аналітиків, що бачать те, чого не помічають інші, і перетворюють відкриті джерела на силу, яка захищає життя та свободу.

На честь тих, хто воює на лінії фронту і в цифровому просторі — адже правда теж вимагає мужності.

Ми дякуємо розвідникам нового часу, які, озброєні знаннями та етикою, роблять невидиме доказовим.

Хай ця книга стане компасом у морі фактів і маяком у нічному штормі даних — щоб кожна іскра істини знаходила шлях до дії. Бо інформація в відповідальних руках — це сила, що оберігає гідність і наближає перемогу.

ЗМІСТ

TABLE OF CONTENTS

ПЕРЕДМОВА

Сьогоднішні виклики у сфері безпеки вимагають не лише технічних рішень, а й підготовлених фахівців, які здатні працювати з інформацією, аналізувати ризики та підтримувати управлінські рішення. У гібридній війні кіберпростір також стає ключовим полем бою, де агресор використовує відкриті джерела, соціальні мережі, фейкові наративи та кібератаки для впливу на державу, суспільство та окремих громадян. У таких умовах знання OSINT – це не просто професійні навички, а елемент національної стійкості.

OSINT – це не просто пошук. Це здатність розпізнати загрозу в інформаційному шумі, виявляти вразливість до того, як вона стане проблемою, і підтримувати рішення, які рятують життя.

Цей навчальний посібник створено для працівників сектору безпеки, оборони та правопорядку, а також для тих, хто проходить професійну підготовку. Його завдання – надати системні знання з OSINT, навчити працювати з інформацією з відкритих джерел, перевіряти її достовірність, виявляти ризики та формувати аналітичні продукти, які можуть бути використані у практичній діяльності. У руках підготовленого фахівця OSINT перетворюється на інструмент випереджального реагування, доказової сили та професійної доброчесності.

Цей навчальний посібник створено для тих, хто прагне не просто оволодіти інструментами OSINT, а розуміти їхню силу, етику та стратегічне значення. Його мета – навчити бачити більше, мислити глибше, діяти точніше.

Посібник охоплює ключові терміни, методи, приклади та алгоритми, які можуть бути застосовані в реальних умовах. Він враховує законодавчі рамки, професійну практику та обмежені ресурси, з якими стикаються наші інституції. Це робить його практичним інструментом для підготовки фахівців, здатних діяти в умовах гібридної війни.

FOREWORD

Today's security challenges require not only technical solutions but also well-trained professionals capable of working with information, analyzing risks, and supporting decision-making processes. In hybrid warfare, cyberspace has also become a key battlefield, where the aggressor uses open sources, social media, disinformation narratives, and cyberattacks to influence the state, society, and individual citizens. In such conditions, OSINT knowledge is not just a professional skill – it is an element of national resilience.

OSINT is not merely about searching. It is the ability to detect threats within information noise, identify vulnerabilities before they become problems, and support decisions that save lives.

This training manual is intended for professionals in the security, defense, and law enforcement sectors, as well as for those undergoing professional preparation. Its purpose is to provide structured knowledge of OSINT, teach how to work with open-source information, verify its reliability, identify risks, and produce analytical outputs applicable in real-world operations. In the hands of a trained specialist, OSINT becomes a tool for proactive response, evidentiary strength, and professional integrity.

This manual is designed for those who seek not only to master OSINT tools but also to understand their power, ethical implications, and strategic value. Its goal is to teach how to see more, think deeper, and act with greater precision.

The manual covers key terms, methods, examples, and algorithms that can be applied in practice. It takes into account legal frameworks, professional standards, and the resource constraints faced by our institutions. This makes it a practical tool for preparing specialists capable of operating effectively in the context of hybrid warfare.

The war continues. And this manual is a contribution to the future – where

Війна триває. І цей посібник – вклад у майбутнє, де аналітика стає основою стійкості, а знання – щитом держави.

analytics becomes the foundation of resilience, and knowledge becomes the shield of the state.

Сергій Демедюк, доктор філософії в галузі права

заступник секретаря Ради національної безпеки і оборони України

Serhii Demediuk, PhD

Deputy Secretary National Security and Defense Council of Ukraine

Палантир XXI сторіччя

Як відкриті дані стали інструментом безпеки

У Толкіна королі дивилися в палантири – камені, що показували минуле й майбутнє. Вони не брехали, але могли заплутати того, хто не розумів побаченого. Сьогодні наші палантири – це відкриті дані, супутники, цифрові архіви. Вони показують світ таким, яким він є, але побачити в них істину можуть не всі.

Війна змінила сенс інформації. Вона стала частиною безпеки, а пошук правди – щоденною роботою команди Molfar. Ми документували воєнні злочини з міжнародними партнерами, ідентифікували російських командирів і маршрути постачання, розкривали схеми обходу санкцій, будували системи моніторингу кіберзагроз. Різні історії, але всі вони про одне: відкриті дані допомагають побачити небезпеку ще до того, як вона стає реальністю.

OSINT в Україні виріс із волонтерських і журналістських ініціатив у велику спільноту, що працює поруч із державою. Аналітики, журналісти, дослідники – усі ми з різних середовищ, але нас об'єднує спільна мета: правда і безпека.

Українська спільнота OSINT стала частиною глобальної екосистеми розвідки у відкритих джерелах. Molfar співпрацює з колегами зі США, Литви, Польщі, Великої Британії – ми обмінюємося аналітиками, методиками, інструментами. За цією співпрацею стоять етика і культура, тому що робота з відкритими даними має супроводжуватись юридичною і моральною відповідальністю.

Molfar – один із флагманів вітчизняної OSINT-індустрії. Щодня ми використовуємо інструменти, описані в цьому виданні, і бачимо, як результати нашої роботи впливають на прийняття важливих рішень. Працюючи з відкритими реєстрами, цифровими слідами, соціальними мережами, та супутниковими знімками ми розуміємо, що кожен наш звіт – це не просто технічний результат процесу пошуку та аналізу, а й документ, що потенційно матиме юридичні наслідки. В книзі окремо розглянуто судову практику, допустимість електронних доказів, територіальну юрисдикцію OSINT, а також використання даних з Deep Web і Dark Web. Це не лише

Palantír of the 21st Century

How Open Data Became a Security Tool

In Tolkien's world, kings gazed into palantírs – stones that revealed the past and future. They didn't lie, but they could mislead those who failed to understand what they saw. Today, our palantírs are open data, satellites, and digital archives. They show the world as it is, but not everyone can discern the truth within them.

War has changed the meaning of information. It has become part of national security, and the search for truth is now the daily work of the Molfar team. We have documented war crimes with international partners, identified russian commanders and supply routes, uncovered sanction evasion schemes, and built systems to monitor cyber threats. These are different stories, but they share a common thread: open data helps detect danger before it becomes reality.

OSINT in Ukraine has grown from volunteer and journalistic initiatives into a broad community working alongside the state. Analysts, journalists, researchers – we come from different backgrounds, but we share a common goal: truth and security.

The Ukrainian OSINT community is now part of the global open-source intelligence ecosystem. Molfar collaborates with colleagues from the United States, Lithuania, Poland, and the Great Britain. We exchange analysts, methodologies, and tools. This cooperation is grounded in ethics and culture, because working with open data requires both legal and moral responsibility.

Molfar is one of the leading players in Ukraine's OSINT industry. Every day, we use the tools described in this publication and see how our work influences critical decision-making. Whether working with public registries, digital traces, social media, or satellite imagery, we understand that each report is not just a technical output—it is a document that may carry legal consequences. This book explores judicial practice, the admissibility of electronic evidence, territorial jurisdiction in OSINT, and the use of data from the Deep Web and Dark Web. It offers not only theoretical insights but also practical guidance for investigators, prosecutors,

теоретична інформація а й практичний орієнтир для слідчих, прокурорів, суддів, що працюють в правовій площині.

Міжнародний контекст – ще один важливий вимір. Сьогодні комерційні аналітичні платформи – від великих технологічних компаній, як-от Microsoft, Google чи Recorded Future, до незалежних європейських розробників – інтегруються у завдання національної безпеки, допомагаючи державам реагувати швидко і точно. Україна вже не просто наздоганяє – вона формує тренди. Важливим є, що у виданні детально описано глобальні стандарти, кейси, практики. Тут представлено трансформацію OSINT у світі, надано приклади інтеграції в оборонні системи, автоматизацію через смарт-контракти, використання AutoML та LLM-моделей.

У книзі сформульована системна база, що охоплює чотири рівні OSINT-аналітики: стратегічний, методологічний, інструментальний та правовий. Така структура відповідає потребам держави, бізнесу, освіти та громадянського суспільства. Вона дозволяє одночасно мислити на рівні національної безпеки, будувати процеси збору та перевірки даних, опановувати інструменти та фреймворки, а також розуміти юридичні межі допустимого. Це важливо – бо OSINT не може існувати без етики, правової легітимності та професійної відповідальності.

Видання також має освітню місію. Воно створене як навчальна платформа для підготовки нової генерації OSINT-фахівців – аналітиків, слідчих, кіберекспертів, журналістів-розслідувачів. Тут є все: від базових інструментів Python і налаштування безпечного середовища до складних сценаріїв фінансової аналітики, цифрової криміналістики та штучного інтелекту. Робота авторського колективу за участю та редакцією Сергія Демедюка – це прикладний посібник, що допоможе сформувати нову культуру роботи з відкритими даними.

Можливо, саме ця книга допоможе вам дивитися у свій, вже сучасний, палантир. І не втрачати з поля зору головне: правду.

Артем Старосєк,

засновник агенції приватної розвідки Molfar

and judges working within the legal domain.

The international context is another key dimension. Today, commercial analytical platforms – from major tech companies like Microsoft, Google, and Recorded Future to independent European developers – are being integrated into national security tasks, helping governments respond quickly and accurately. Ukraine is no longer catching up – it is setting trends. This publication provides detailed coverage of global standards, case studies, and practices. It presents the transformation of OSINT worldwide, including examples of integration into defense systems, automation via smart contracts, and the use of AutoML and LLM models.

The book outlines a structured foundation encompassing four levels of OSINT analytics: strategic, methodological, instrumental, and legal. This framework meets the needs of government, business, education, and civil society. It enables thinking at the level of national security, building processes for data collection and verification, mastering tools and frameworks, and understanding the legal boundaries of what is permissible. This is essential – because OSINT cannot exist without ethics, legal legitimacy, and professional accountability.

This publication also serves an educational purpose. It is designed as a training platform for the next generation of OSINT professionals – analysts, investigators, cybersecurity experts, and investigative journalists. It covers everything: from basic Python tools and secure environment setup to advanced scenarios in financial analytics, digital forensics, and artificial intelligence. The work of the author team, with the participation and editing of Serhii Demydiuk is a practical guide that will help shape a new culture of working with open data.

Perhaps this book will help you look into your own, modern-day palantír – and keep sight of what matters most: the truth.

Artem Starosiek,

Founder of Molfar Private Intelligence Agency

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.

Leonard STRASHNOY – University of California, Los Angeles (USA);

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);*

Сергій БОРТНИК – доктор юридичних наук, професор – *Харківський національний університет внутрішніх справ;*

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

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

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

Олександр Олександрович КОРИСТІН – Служба з питань інформаційної безпеки та кібербезпеки Апарату РНБО України;

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;*

Ярослав ЛІХОВІЦЬКИЙ – доктор юридичних наук, професор – *Ужгородський національний університет;*

Євгеній ПАНЧЕНКО – Департаменту міжнародного поліцейського співробітництва НПУ;

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

Христина ПОДИРЯКО – Головне слідче управління Національної поліції України;

Роман РАСКЕВИЧ – Державна прикордонна служба України;

Станіслав САМОЙЛОВ – кандидат юридичних наук – *Департамент кіберполіції Національної поліції України;*

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

Ганна СОБКО – доктор юридичних наук, професор – *Одеський державний університет внутрішніх справ;*

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

Дмитро ШЕВЧУК – Головне слідче управління Національної поліції України;

Олександр ШУКЛІН – Департамент кіберполіції Національної поліції України.

"Вивчення OSINT – це не лише про інструменти. Це про здатність мислити ясно, діяти відповідально й бачити крізь хаос" –

Авторська формула

ВСТУП

Передумови та обґрунтування

Сучасна система безпеки України перебуває у стані постійної напруги через комплекс внутрішніх та зовнішніх викликів: триваючу воєнну агресію проти нашої держави, гібридні інформаційні атаки, зростання масштабів кіберзлочинності, транснаціональну організовану злочинність та інші форми протиправної діяльності. Ці виклики розвиваються на тлі стрімкої цифровізації суспільства, що призводить до появи нових каналів комунікації, обміну даними і водночас нових способів приховування злочинної активності.

У цих умовах ефективність правоохоронних органів визначається здатністю діяти **проактивно:** не лише реагувати на вчинені правопорушення, а й завчасно виявляти загрози, прогнозувати їх розвиток і запобігати негативним наслідкам. Ключовим підходом, який підтримує таку трансформацію, є модель правоохоронної діяльності, керованої аналітичною розвідкою (*Intelligence-led Policing, ILP*), що ставить у центр процесу управлінські та процесуально значущі рішення, засновані на комплексному аналізі даних.

Розвідка з відкритих джерел (*Open-Source Intelligence, OSINT*) у цій моделі посідає особливе місце. Вона дає можливість:

оперативно отримувати релевантну інформацію з величезних масивів відкритих джерел – від офіційних державних реєстрів до соціальних мереж і спеціалізованих платформ;

комплексно поєднувати відкриті дані з іншими видами розвідувальної та криміналістичної інформації;

аналітично обробляти зібрані дані для формування профілів загроз, оцінки ризиків, виявлення трендів та встановлення прихованих зв'язків;

Background and rationale

Ukraine's current security system operates under constant pressure due to a combination of internal and external challenges: the ongoing military aggression against the state, hybrid information attacks, the growing scale of cybercrime, transnational organized crime, and other forms of unlawful activity. These threats are evolving against the backdrop of rapid digitalization, which has led to the emergence of new communication channels, data exchange mechanisms, and, simultaneously, new methods of concealing criminal activity.

In this context, the effectiveness of law enforcement agencies depends on their ability to act proactively – not only responding to committed offenses but also identifying threats in advance, forecasting their development, and preventing negative consequences. A key approach supporting this transformation is the Intelligence-led Policing (ILP) model, which places data-driven, management-level and procedurally significant decisions at the center of law enforcement operations.

Within this model, Open-Source Intelligence (OSINT) plays a critical role. It enables:

operationally access to relevant information from vast volumes of open sources – from official government registries to social media and specialized platforms;

combine of open data with other types of intelligence and forensic information;

analytical processing of collected data to build threat profiles, assess risks, identify trends, and uncover hidden connections;

evidentiary documentation of

доказово фіксувати інформацію для використання у кримінальному провадженні, із дотриманням процесуальних та етичних стандартів.

З огляду на реалії воєнного часу та постійні гібридні атаки, OSINT стає не лише інструментом підтримки досудового розслідування, а й невід'ємним елементом національної оборони та безпеки. Пошук і перевірка фактів, ідентифікація фейкових наративів, моніторинг кібератак, документування порушень прав людини, встановлення місцезнаходження зниклих безвісти – усе це напрямки, де відкриті дані виконують критичну функцію.

Реалізація знань і навичок, викладених у посібнику, сприятиме створенню в Україні сильної, адаптивної та етично вивіреної культури OSINT, де інформація з відкритих джерел стає не просто даними, а стратегічною перевагою у боротьбі за безпеку та свободу.

Мета та особлива роль

Цей навчальний посібник створено як системний, практико-орієнтований інструмент підготовки фахівців, здатних упевнено застосовувати методи та інструменти відкритої розвідки (OSINT) у межах моделі правоохоронної діяльності, керованої аналітичною розвідкою (Intelligence-led Policing, ILP). Його мета – сформувати у слухачів не лише загальне розуміння концепції OSINT, а й надати відпрацьовані на практиці алгоритми роботи з відкритими джерелами, які можна відразу інтегрувати у реальні робочі процеси.

Посібник виходить з того, що ефективність OSINT визначається не кількістю використаних інструментів, а чіткістю і послідовністю дій аналітика. Саме тому матеріал викладено так, щоб читач міг від початкового етапу – постановки завдання, формулювання пошукових критеріїв і відбору джерел – пройти крізь усі ключові фази: збір та збереження даних із застосуванням сучасних цифрових інструментів, багаторівневу верифікацію, аналітичне опрацювання з використанням візуалізацій та інтеграцію отриманих результатів у звітність, придатну для управлінських і процесуальних рішень.

Особлива роль цього посібника полягає у поєднанні теоретичних основ OSINT із конкретними практичними сценаріями, де кожна методика підкріплена прикладами

information for use in criminal proceedings, in compliance with procedural and ethical standards.

Given the realities of wartime and ongoing hybrid attacks, OSINT is not only a tool for supporting pre-trial investigations – it is also an essential component of national defense and security. Fact-checking, identifying disinformation narratives, monitoring cyberattacks, documenting human rights violations, and locating missing persons are all areas where open data performs a critical function.

Applying the knowledge and skills presented in this manual will contribute to the development of a strong, adaptive, and ethically grounded OSINT culture in Ukraine – where open-source information becomes not just data, but a strategic asset in the pursuit of security and freedom.

Objective and added value

This training manual has been developed as a systematic, practice-oriented tool for preparing specialists capable of confidently applying open-source intelligence (OSINT) methods and tools within the framework of Intelligence-led Policing (ILP). Its goal is not only to provide learners with a general understanding of the OSINT concept but also to offer tested, practical algorithms for working with open sources that can be immediately integrated into real operational workflows.

The manual is based on the principle that OSINT effectiveness is determined not by the number of tools used, but by the clarity and consistency of the analyst's actions. For this reason, the material is structured to guide the reader through all key phases – from task definition, formulation of search criteria, and source selection to data collection and storage using modern digital tools, multi-level verification, analytical processing with visualizations, and integration of results into reports suitable for managerial and procedural decision-making.

A distinctive feature of this manual is its combination of OSINT theory with concrete practical scenarios, where each method is supported by examples of current tools – from search operators and social media monitoring platforms

використання актуальних інструментів – від пошукових операторів і платформ моніторингу соціальних медіа до сервісів геолокаційного аналізу та автоматизованого збору даних. Кожен алгоритм подано як готову технологічну карту дій, що враховує часові обмеження, ризики операційної безпеки та можливі контрзаходи з боку противника.

Додатково, навчальний посібник побудовано таким чином, щоб він був однаково корисним як для початківця, який лише опановує основи відкритої розвідки, працюючи з перевіреними й простими у використанні інструментами та класичними методами пошуку й аналізу, так і для більш досвідченого аналітика, який прагне підняти свій рівень, опановуючи програмний код на Python для автоматизації збору та обробки даних, а також безкодове програмування із застосуванням сучасних платформ штучного інтелекту. Така побудова дозволяє поступово переходити від базових процедур до створення власних автоматизованих рішень і складних аналітичних сценаріїв, забезпечуючи гнучкість навчання та максимальну прикладну цінність матеріалу для будь-якого рівня підготовки.

Посібник орієнтований на формування універсальної компетентності: слухач після його опрацювання зможе у будь-якому середовищі – чи то у підрозділі кримінального аналізу, чи у команді OSINT-журналістів, чи в структурі інформаційної безпеки – діяти швидко, методично і безпомилково, використовуючи сучасні інструменти максимально ефективно. Таким чином, видання стає не лише навчальною базою, а й операційним довідником, який можна відкрити у критичний момент і отримати чіткий, покроковий алгоритм для досягнення результату.

to geolocation analysis services and automated data collection systems. Each algorithm is presented as a ready-to-use technological action map, taking into account time constraints, operational security risks, and potential countermeasures by adversaries.

Additionally, the manual is designed to be equally useful for beginners – those just learning the basics of open-source intelligence using reliable and user-friendly tools and classical search and analysis methods – and for more experienced analysts seeking to advance their skills by mastering Python code for data collection and processing automation, as well as no-code programming using modern artificial intelligence platforms. This structure allows for a gradual transition from basic procedures to the creation of custom automated solutions and complex analytical scenarios, ensuring flexible learning and maximum practical value for any level of expertise.

The manual is aimed at developing universal competence: upon completion, the reader will be able to operate effectively in any environment – whether in a crime analysis unit, an OSINT journalism team, or an information security structure – acting quickly, methodically, and accurately while using modern tools to their full potential. Thus, the publication serves not only as a training resource but also as an operational reference guide that can be opened in a critical moment to access a clear, step-by-step algorithm for achieving results.

Олександр КОРИСТІН
доктор юридичних наук, професор

Oleksandr KORYSTIN
DSc Law, Professor

«Там, де процес структурований, а ризики передбачені — аналітика стає не загрозою, а гарантією безпеки»

- Авторська формула

У розвідці з відкритих джерел перший крок – не пошук, а захист. Захист себе, захист об'єкта дослідження, захист довіри до процесу. Як зазначав Брюс Шнайєр, експерт з кібербезпеки:

«Безпека – це не продукт, а процес. І він починається з усвідомлення ризику».

OSINT – це не лише доступ до інформації, а відповідальність за її обробку. Анонімність – не втеча, а інструмент етичного дистанціювання. Технічна грамотність – не опція, а передумова безпечної аналітики.

Ця частина посібника – про те, як налаштувати себе і своє середовище так, щоб розвідка не стала загрозою. Бо там, де процес структурований, а ризики передбачені, народжується не просто ефективність – народжується довіра до аналітика.

ПРОЦЕС, АНОНІМНІСТЬ, БЕЗПЕКА

ЧАСТИНА І

РОЗДІЛ 1

ПОПУЛЯРНО ПРО OSINT: ЯК ШУКАТИ ДУМАТИ І НЕ ЗАГУБИТИСЯ

Олександр КОРИСТІН

ВСТУП ДО OSINT: ЯК ПЕРЕТВОРИТИ ІНФОРМАЦІЮ НА РОЗВІДКУ

Розвідка з відкритих джерел (OSINT – Open Source Intelligence) є фундаментальним інструментом сучасної аналітики, кібербезпеки та стратегічного планування. Вона базується на зборі, перевірці, аналізі та інтерпретації інформації, що доступна без обмежень – тобто у відкритому доступі. Це можуть бути медіа, соціальні мережі, бази даних, відео, карти, форуми, офіційні документи, наукові публікації тощо.

OSINT не просто відповідає на запитання. Вона дозволяє бачити ширше, діяти точніше і прогнозувати глибше. Але щоб зрозуміти її силу, потрібно розрізнити два ключові поняття – *інформацію та розвідку*.

Інформація: сировина для аналітики

Інформація – це все, що нас оточує. Вона хаотична, фрагментарна, часто суперечлива. Це новинні заголовки, твіти, відео, пости, коментарі, документи, геолокаційні мітки. У світі OSINT інформація – це початкова точка, але не кінцева мета. Як сира їжа, вона потребує обробки, перевірки і осмислення. Без цього вона залишається просто шумом.

Розвідка: результат осмислення

Розвідка – це вже результат інтелектуальної роботи. Це структурована, перевірена, контекстуалізована інформація, яка має практичну цінність. Вона дозволяє приймати рішення, формувати стратегії, виявляти ризики, прогнозувати сценарії. Якщо інформація – це набір інгредієнтів, то розвідка – це страва, яку можна подати, оцінити і використати.

Трансформація: шлях від даних до рішень

Процес перетворення інформації на розвідку – це серцевина OSINT. Він не є автоматичним. Це послідовна, критично осмислена діяльність, яка вимагає навичок, досвіду і етичної відповідальності. Цей процес можна умовно поділити на п'ять етапів:

Етап	Суть процесу
Збір	Виявлення релевантних джерел: медіа, соцмережі, бази даних, карти, відео
Перевірка	Оцінка достовірності, джерельної надійності, актуальності, контексту
Аналіз	Виявлення закономірностей, аномалій, зв'язків, прихованих сигналів
Синтез	Об'єднання фрагментів у цілісну картину, формування гіпотез і висновків
Інтерпретація	Оцінка значення отриманих інсайтів для прийняття рішень, дій, стратегій

Кожен етап – це не просто технічна дія, а аналітичне мислення. Наприклад:

Збір – це не просто пошук, а вміння бачити потенціал у джерелах, які інші ігнорують.

Перевірка – це навичка відрізняти факт від маніпуляції, розпізнавати фейки, виявляти джерельні конфлікти.

Аналіз – це здатність побачити за даними історію, яку вони розповідають, навіть якщо вона неочевидна.

Синтез – це момент, коли окремі фрагменти складаються у логічну, переконливу картину.

Інтерпретація – це етап, де розвідка стає дієвим інструментом: для реагування, планування, комунікації.

OSINT – це не просто технологія. Це культура мислення, яка поєднує етику, аналітику, стратегічне бачення і глибоке розуміння людського контексту.

ПАСИВНИЙ ТА АКТИВНИЙ OSINT: МЕЖІ СПОСТЕРЕЖЕННЯ І ВЗАЄМОДІЇ

У практиці OSINT важливо розуміти не лише джерела інформації, а й спосіб взаємодії з ними. Існує два основних підходи – пасивний та активний OSINT. Вони є частинами одного процесу, але мають різні етичні, технічні та операційні наслідки. Вибір між ними залежить від мети дослідження, політики організації та рівня ризику.

Пасивний OSINT: спостереження без сліду

Пасивний OSINT – це збір інформації без прямої взаємодії з об'єктом дослідження. Аналітик діє як спостерігач: переглядає відкриті профілі, читає публікації, аналізує метадані, досліджує карти, форуми, бази даних. Він не залишає цифрового сліду, не вступає в контакт, не змінює поведінку цілі.

Цей підхід є безпечним, етично нейтральним і широко застосовуваним в аналітиці, журналістиці, дослідницьких проєктах. Його переваги:

- *мінімальний ризик викриття;*
- *відповідність більшості внутрішніх політик;*
- *можливість масштабного моніторингу.*

Проте пасивний OSINT має обмеження: він не дозволяє отримати інформацію, що прихована за умовною *«взаємодією»* – наприклад, у закритих групах або приватних переписках.

Пасивний OSINT – кейси спостереження без взаємодії

Кейс 1: Моніторинг дезінформації у Facebook

Ситуація: Аналітик кіберполіції досліджує поширення фейкових новин про гуманітарну допомогу.

Дії: *Збір публічних постів із відкритих сторінок.*

Аналіз хештегів, часу публікацій, геолокації.

Виявлення повторюваних джерел та шаблонів повідомлень.

Результат: Визначено мережу ботів, які поширюють однакові меседжі з різних акаунтів.

Кейс 2: Вивчення цифрового сліду підозрюваного

Ситуація: Потрібно оцінити онлайн-активність особи, яка фігурує у справі про кіберзлочин.

Дії: *Перегляд публічних профілів у LinkedIn, GitHub, Twitter.*

Аналіз коментарів на форумах, участі в онлайн-спільнотах.

Збір метаданих із зображень, що були опубліковані.

Результат: Встановлено зв'язок між акаунтами, виявлено місце роботи та технічні навички.

15. Яка перевага OSINT дозволяє діяти оперативно у кризових ситуаціях?
а) Обмежений доступ до джерел
б) Залежність від агентів
в) Висока вартість
г) Актуальність у реальному часі

РОЗДІЛ 2

БЕЗПЕКА РОЗСЛІДУВАНЬ У ЦИФРОВОМУ СЕРЕДОВИЩІ: ЯК НЕ ЗАСВІТИТИСЯ, КОЛИ ШУКАЄШ

Наталія ЦЮПРИК

У світі OSINT, де все начебто відкрито, найбільша загроза – це те, що відкритим можете стати ви. Анонімність аналітика – не просто технічна опція, а стратегічна необхідність. Якщо ви хочете досліджувати, не привертаючи уваги, діяти ефективно і безпечно, вам потрібно навчитися бути *«невидимим»* у цифровому середовищі.

OSINT-дослідження – це завжди про збір даних. Але якщо об'єкт розслідування дізнається, що його моніторять, він може швидко змінити поведінку, зачистити сліди, закрити профілі, видалити пости або навіть знищити докази. Це не просто ускладнює роботу – це може повністю зруйнувати розслідування ще до того, як ви зберете достатньо інформації. Тому збереження анонімності – це не *«бажано»*, а *«обов'язково»*.

Анонімність також захищає самих аналітиків. У багатьох випадках об'єкти OSINT – це не просто користувачі соцмереж, а хакери, злочинні угруповання, радикальні активісти. Якщо вони дізнаються, хто саме їх досліджує, можуть спробувати атакувати у відповідь – технічно або навіть фізично. Тому захист особистості, пристроїв і каналів зв'язку – це частина професійної етики і безпеки.

І ще один важливий аспект – юридичний. У деяких країнах навіть ненавмисне розкриття факту розслідування може мати наслідки. Ви можете порушити закон, навіть не усвідомлюючи цього. Анонімність – це також спосіб уникнути юридичних помилок і етичних дилем.

ЯК ВАС МОЖУТЬ «ЗАСВІТИТИ»: ТИПОВІ РИЗИКИ І ЯК ЇХ УНИКАТИ

IP-адреса: цифровий слід, який веде до вас

Кожен пристрій, підключений до інтернету, має IP-адресу – унікальний ідентифікатор, який дозволяє сайтам бачити, звідки ви заходите. Якщо ви не використовуєте VPN або Tor, ваша реальна IP-адреса буде зафіксована. Це означає, що вас можна ідентифікувати за місцем проживання, провайдером, навіть містом.

Щоб цього уникнути, використовуйте VPN-сервіси з перевіреною політикою конфіденційності. Вони створюють *«тунель»* між вами і сайтом, приховуючи вашу реальну адресу. Але пам'ятайте: не всі VPN однаково надійні. Деякі з них ведуть журнали активності, навіть якщо заявляють протилежне.

Відбитки браузера: вас видає навіть те, як виглядає ваш екран

Ваш браузер – це набір унікальних параметрів: роздільна здатність, мова, встановлені плагіни, шрифти, тип пристрою. Усе це формує *«цифровий відбиток пальця»*, за яким вас можна впізнати навіть без IP-адреси.

Цей відбиток зберігається на серверах, і якщо ви заходите на сайт кілька

разів – вас можуть ідентифікувати, навіть у режимі інкогніто. Тому важливо використовувати браузери, орієнтовані на конфіденційність, наприклад Tor або Brave, мінімізувати плагіни і змінювати налаштування.

Перевір себе: зайди на privacy.net/analyzer – і побачиш, скільки про тебе вже знає браузер (*рис.1*). Це не страшилка – це реальність.

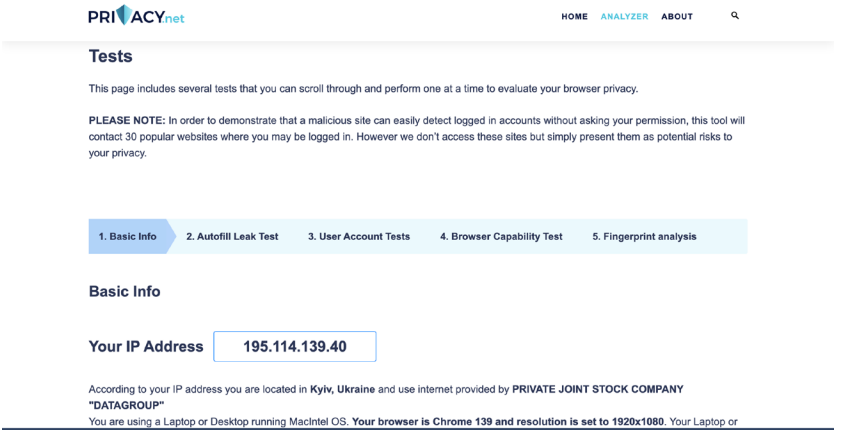


Рисунок 1. Результати тесту на privacy.net/analyzer

Надмірна віра в технології: VPN і Tor – не броня

Багато хто думає: «Я використовую VPN – отже, я в безпеці». Але це не зовсім так. Деякі VPN-сервіси реєструють вашу активність, зберігають IP-адреси, часові мітки. А Tor, хоч і потужний, не захищає від усіх форм відстеження – особливо якщо проти вас працює державна структура або технічно підготовлена група.

Тому не покладайтеся на один інструмент. Комбінуйте VPN, Tor, браузери з конфіденційністю, змінюйте шаблони поведінки. І головне – розумійте, як працює кожен інструмент, і де його слабкі місця.

Файли cookie: дрібні, але нав'язливі

Cookie – це маленькі текстові файли, які сайти залишають у вашому браузері (*рис.2*). Вони запам'ятовують вас, створюють профілі, передають дані між сайтами. І навіть якщо ви очищаєте їх регулярно, компанії використовують більш просунуті методи – дактилоскопію браузера, полотна, поведінкові патерни.

Щоб зменшити ризик, використовуйте розширення для блокування трекерів, очищуйте cookie після кожного сеансу, не повторюйте шаблони поведінки.

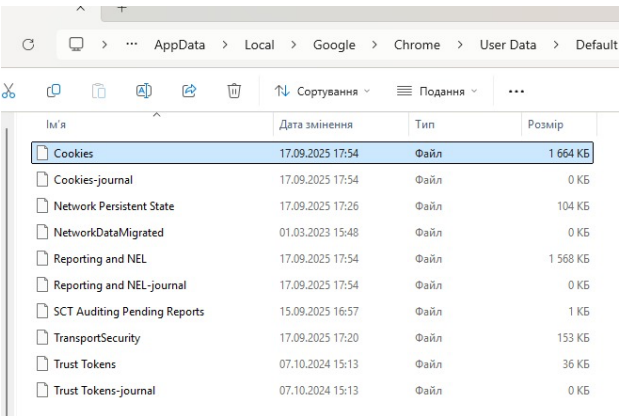


Рисунок 2. Файли cookie зберігаються в різних місцях, але можуть розкривати досить багато інформації

11. Що таке претекстинг і чому він важливий для побудови онлайн-персони?
12. Які елементи повинна містити біографія sock puppet-персони?
13. Який сервіс дозволяє створити унікальне фото неіснуючої особи для sock puppet?
14. Чому не можна використовувати особисту електронну пошту або номер телефону для sock puppet?
15. Які сервіси рекомендовано для створення анонімної електронної адреси та тимчасових акаунтів?
16. Які месенджери забезпечують зашифровану комунікацію для sock puppet?
17. Які дії слід виконати після завершення роботи з burner-пристроєм?
18. Як правильно документувати дії sock puppet-персони для звітності та безпеки?
19. Які етичні обмеження слід враховувати при використанні sock puppet?
20. Як гендерна динаміка може вплинути на сприйняття sock puppet-персони в онлайн-середовищі?

РОЗДІЛ 3

АРХІТЕРТУРА СУЧАСНОЇ КІБЕРБЕЗПЕКИ ОСОБИ ТА ОРГАНІЗАЦІЇ

Ганна СОБКО

Цифровий простір став невід'ємною частиною нашого життя. Ми працюємо, навчаємось, спілкуємось і приймаємо рішення онлайн. Кожна дія залишає слід, а кожен слід – це потенційна вразливість. У світі, де інформація стала новою валютою, захист цифрової ідентичності – це не просто технічна задача, а стратегічна необхідність. Кіберзагрози еволюціонують, стають складнішими і менш помітними. Вони можуть бути спрямовані як проти окремої особи, так і проти цілої організації. Саме тому знання про OSINT – розвідку з відкритих джерел – є ключовим інструментом не лише для виявлення загроз, а й для побудови системи захисту.

РОЛЬ OSINT У ЗАХИСТІ ОСОБИСТОСТІ ТА ОРГАНІЗАЦІЇ

OSINT – це систематичний збір і аналіз відкритих даних для прийняття обґрунтованих рішень. Джерела включають новини, публічні реєстри, соціальні мережі, форуми, технічні метадані, цифрові сліди.

Роль OSINT в кібербезпеці є комплексною. Для приватної особи OSINT – це спосіб побачити себе очима зовнішнього світу, а також захисту особистої ідентичності в Інтернеті. Він дозволяє виявити надмірно відкриту інформацію, оцінити ризики і вжити заходів для захисту. Це може бути профіль у соцмережі, фото з геолокацією, коментарі на форумах або навіть старі публікації, які вже втратили актуальність, але залишилися доступними. Методи OSINT можуть допомогти виявити вразливі місця у особистій цифровій сутності.

Для організації OSINT – це інструмент стратегічного моніторингу. Він допомагає виявляти технічні вразливості, аналізувати поведінку потенційних зловмисників, відстежувати згадки про бренд, оцінювати репутаційні ризики. Це основа для побудови системи кіберзахисту, яка реагує не лише на атаки, а й на сигнали, що передують їм.

ПЕРЕВАГИ ПРОАКТИВНИХ OSINT-ДОСЛІДЖЕНЬ ДЛЯ КІБЕРБЕЗПЕКИ

У сфері кібербезпеки проактивність – це не просто перевага, це необхідність. OSINT дозволяє діяти на випередження, виявляючи загрози ще до того, як вони набудуть форми атаки. Це дає змогу не лише захищатися, а й прогнозувати ризики, адаптувати стратегії та зберігати контроль над ситуацією.

Постійний моніторинг відкритих джерел – це спосіб бачити те, що бачать зловмисники. Організація, яка регулярно аналізує інформаційне поле, здатна виявити витоки даних, підозрілі згадки, зміну поведінки у ворожих спільнотах. Це дозволяє вчасно реагувати, не чекаючи інциденту.

Проактивний OSINT також відіграє ключову роль у розвідувальному аналізі загроз. Він допомагає зрозуміти, хто стоїть за потенційною атакою, які методи використовуються, яка мотивація лежить в основі дій. Це знання дозволяє будувати не просто технічний захист, а стратегічну модель реагування.

Ще одна важлива перевага – управління ризиками. Кіберзагрози змінюються щодня. Те, що було актуальним вчора, сьогодні може бути застарілим. OSINT дозволяє постійно оновлювати карту ризиків, коригувати політики безпеки, адаптувати інструменти захисту. Це створює динамічну систему, здатну витримати тиск змін.

І нарешті, проактивна позиція – це показник зрілості організації. Це демонстрація готовності не лише реагувати, а й передбачати. Це також гарантія стабільності для фахівців, які володіють навичками OSINT. У світі, де інформація – це сила, вміння працювати з відкритими джерелами – це форма професійної стійкості.

ОСОБИСТА ЦИФРОВА ГІГІЄНА ТА OSINT

Цифрова гігієна – це сукупність практик, які допомагають зберігати контроль над власною онлайн-присутністю. Вона починається з усвідомлення того, що кожна дія в мережі залишає слід. Цей слід – це набір даних, які можуть бути зібрані, проаналізовані та використані як на користь, так і проти вас.

Ваш цифровий слід охоплює все: активність у соціальних мережах, участь у форумах, онлайн-покупки, коментарі, фото, геолокацію, історію пошуку, навіть метадані у файлах. І це не обмежується лише комп'ютером – смартфон, планшет, розумний годинник, голосові помічники – всі вони генерують дані, які можуть бути доступні стороннім особам.

Інструменти OSINT дозволяють скласти повну картину вашої цифрової поведінки. Агрегатори даних, пошукові системи, спеціалізоване програмне забезпечення – усе це використовується для аналізу відкритої інформації. Те, що здається дрібницею, може стати ключем до вашої ідентифікації або до атаки.

Надмірне поширення особистої інформації – одна з найпоширеніших вразливостей. Відкриті профілі, фото з геотегами, публікації про місце роботи чи відпочинку – усе це створює карту вашого життя, доступну будь-кому. Зловмисники використовують ці дані для фішингу, соціальної інженерії, крадіжки особистості або навіть фізичного стеження.

Цифрова гігієна – це не одноразова дія, а постійний процес. Регулярний перегляд налаштувань конфіденційності, очищення історії, обмеження доступу до особистих даних – це базові кроки. Важливо також періодично перевіряти, що про вас можна знайти в Інтернеті, і вчасно реагувати на потенційні витоки.

OSINT у цьому контексті – це не лише інструмент розслідування, а й дзеркало. Він показує, як виглядає ваша цифрова особистість ззовні. І саме це знання дозволяє вам зробити її менш вразливою, більш контрольованою і захищеною.

19. Чому важливо адаптувати стратегію кібербезпеки до нових загроз?
20. Які етичні принципи слід враховувати при використанні OSINT-інструментів?

РОЗДІЛ 4
НАЛАШТУВАННЯ ІНФОРМАЦІЙНО-БЕЗПЕКОВОГО СЕРЕДОВИЩА В РОЗРІЗІ ПРОВЕДЕННЯ OSINT

Карен ІСМАЙЛОВ

У сучасному інформаційному просторі розвідка на основі відкритих джерел (OSINT) відіграє критично важливу роль у правоохоронній сфері. Зважаючи на динамічний розвиток цифрових платформ, збільшення обсягів інформації та всебічну діджиталізацію суспільства, а з ним неминуче і правоохоронної системи, необхідність ефективного проведення OSINT постійно зростає.

Водночас, проведення OSINT без забезпечення належного рівня цифрової гігієни та безпеки може спричинити викриття дослідника, компрометацію інструментів та витік конфіденційної інформації, що створить додаткові ризики для діяльності правоохоронних або дослідницьких структур. Саме тому створення безпекового середовища для проведення OSINT є ключовою умовою ефективної, анонімної та захищеної роботи.

Безпечне середовище OSINT – це сукупність технічних, програмних та організаційних засобів, що забезпечують анонімність, ізольованість та захищеність дослідника на всіх етапах розвідувального процесу.

Далі в цьому розділі ми більш детально, з конкретними алгоритмами дій, торкнемося питань забезпечення безпечного середовища, а зараз тільки зупинимося на основним моментах його побудови для того, щоб сформувалася загальна картина.

Відмічаємо, що все програмне забезпечення, яке ми будемо згадувати повинно бути ліцензоване та своєчасно оновлюватися, а отже, основним пріоритетом налаштування безпекового середовища є запобігання відстеженню активності користувача та його деанонімізації. Тому необхідно на робочому ПК інсталювати операційну систему, встановити антивірусну програму та віртуальну приватну мережу (VPN), браузери, менеджер паролів, шифрування дисків, програму для віртуалізації операційних систем та інше програмне забезпечення (OSINT-інструменти).

Таким чином, дослідник налаштує ізольовану зону (мережу) (Isolated Zone), що буде відповідати підвищеним вимогам до безпеки. Тим самим проведення OSINT буде відбуватися без контакту з реальною інфраструктурою користувача.

Компонентами **ізольованої зони** є:

1. Налаштування віртуальної машини (VM) або фізично відокремлений пристрій;
2. Операційна система з підтримкою ізоляції (Tails, Whonix, Qubes OS);
3. VPN + Tor для подвійної анонімності;
4. Firewall/Sandboxing – жорстке обмеження мережевої активності.
5. Інструменти OSINT: Maltego, Sherlock тощо.

Налаштування ізольованої зони:

1. Встановити VirtualBox.
2. Завантажити Whonix (дві VM: Whonix-Gateway + Whonix-Workstation).
3. Налаштувати Whonix-Gateway – ця VM використовує Tor для трафіку.
4. Налаштувати Whonix-Workstation – VM без прямого інтернет-доступу, все йде через Gateway.
5. Заблокувати доступ Workstation до локальних ресурсів:
    - відключити drag'n'drop;
    - заборонити доступ до основного диску;
    - використати Snapshot режим або Immutable Disk Mode.
6. Встановити OSINT-інструменти у Workstation.

Таким чином, безпекове середовище повинно бути побудоване відповідно до найкращих практик цифрової гігієни та оперативної безпеки (OPSEC), з акцентом на постійне оновлення інструментів, контроль витоку метаданих та застосування шифрування для збереження зібраної інформації.

ОПЕРАЦІЙНІ СИСТЕМИ: ПРИЗНАЧЕННЯ, ПЕРЕВАГИ, ПОРЯДОК ВСТАНОВЛЕННЯ

Робочим інструментом дослідника є персональний комп'ютер. Якщо останній вже був у використанні, то необхідно повністю переінсталювати операційну систему, за умови нового обладнання – встановити нову операційну систему.

Операційна система (ОС) – це комплекс програмних засобів, що забезпечує керування апаратними ресурсами комп'ютера та створює середовище для функціонування прикладного програмного забезпечення. ОС є фундаментальною частиною будь-якої обчислювальної системи, яка координує взаємодію між програмами та фізичними компонентами пристрою.

Призначення операційної системи

1. Керування апаратними ресурсами. ОС здійснює розподіл процесорного часу, оперативної пам'яті, простору на дисках та інших ресурсів між програмами та процесами.
2. Підтримка багатозадачності. ОС дозволяє виконувати кілька програм одночасно шляхом перемикання контексту між процесами (мультипроцесорна та багатопоточна підтримка).
3. Файлова система. ОС організовує, зберігає та захищає дані користувача у вигляді ієрархічної файлової системи, надаючи засоби зчитування, запису, пошуку та захисту інформації.
4. Інтерфейс користувача. Забезпечує взаємодію між користувачем і комп'ютером, зокрема через графічний інтерфейс (GUI) або командний рядок (CLI).

«Архітектура OSINT — це не набір функцій,
а інтелектуальна інфраструктура й
запрошення до відповідального дослідження»
- Авторська формула

У розвідці з відкритих джерел інструмент – це не просто програма, чи засіб, а продовження мислення аналітика. Як зазначав Кевін Мітнік (*Kevin David Mitnick*), легендарний хакер і консультант з безпеки: «*Найсильніша зброя – це не код, а розум, який ним користується.*»

Фреймворки, пошукові системи, метадані, соціальні мережі, Dark Net, реєстри – усе це не набір функцій, а архітектура доступу до фактів, зв'язків і контекстів. Але ефективність залежить не від кількості інструментів, а від здатності бачити за ними сенс.

Майкл Базель (*Michael Bazzell*), фахівець із кібербезпеки та автор методичних посібників з OSINT, доповнюючи акцентує: «*Новий фахівець з OSINT має бути самодостатнім і володіти власними інструментами та ресурсами.*»

Ця частина про те, як технічна грамотність перетворюється на аналітичну силу, як архітектура OSINT вибудовується не з окремих блоків, а з взаємопов'язаних рішень. Тут аналітик не просто користується інструментом, він формує власну екосистему, яка стає не просто середовищем роботи, а простором відповідальності, точності й стратегічного бачення.

АРХІТЕКТУРА OSINT: інструменти, системи, дослідницькі підходи

ЧАСТИНА II

РОЗДІЛ 5

ОПЕРАЦІЙНА БАЗА OSINT: ФРЕЙМВОРКИ, СЕРВІСИ, МОБІЛЬНІ РІШЕННЯ

Карен ІСМАЙЛОВ
Олександр ШУКЛІН

ФРЕЙМВОРКИ OSINT-ІНСТРУМЕНТІВ

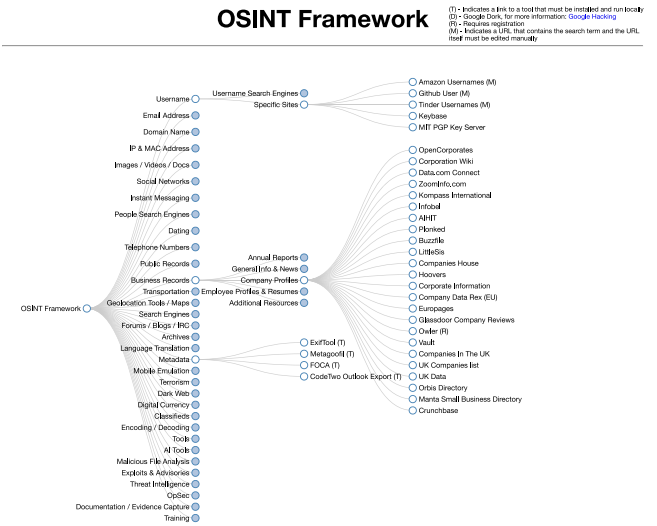
У процесі дослідження прикладних аспектів використання інформаційно-комунікаційних технологій у сфері відкритої розвідки нами було здійснено систематичний відбір інструментів, що відповідають ключовим критеріям: відкритий вихідний код, безкоштовний доступ для користувачів, доведена ефективність на практиці та наявність актуальної підтримки спільнотою або розробником. Такий підхід ґрунтується на принципах наукової обґрунтованості та реплікованості досліджень, що дозволяє забезпечити незалежність від комерційних платформ і зберегти високий рівень адаптивності інструментарію до умов, які змінюються.

Слід зауважити, що цифрове середовище є динамічним, а життєвий цикл навіть найбільш популярного програмного забезпечення може бути непередбачуваним – припинення розробки, втрата сумісності з оновленими системами чи необхідність встановлення бібліотек, які можуть бути несумісними з технічними ресурсами дослідника. У цьому контексті критично важливим є формування у фахівця з відкритої розвідки не лише компетенцій із застосування окремих інструментів, а й розвиток методологічної гнучкості, що передбачає вміння швидко орієнтуватися у новому програмному середовищі, здійснювати порівняльний аналіз альтернативних рішень та формувати ефективні програмні стеки відповідно до завдань дослідження.

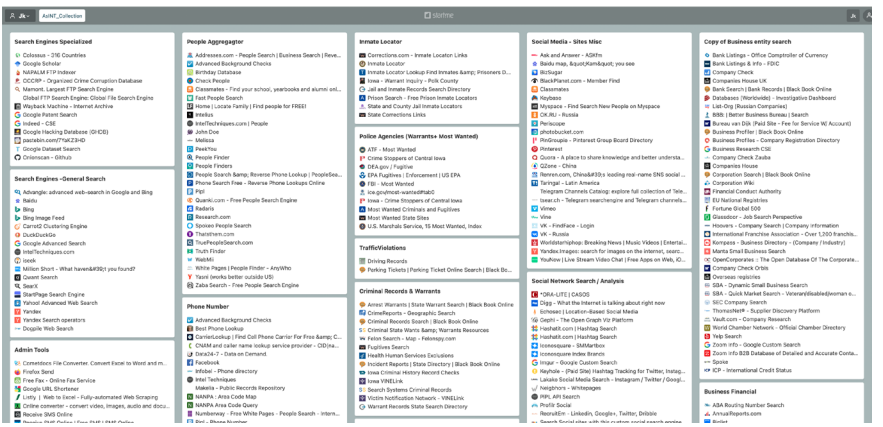
Фреймворки OSINT-інструментів репрезентують структуровані програмно-методологічні комплекси, призначені для систематичного збору, обробки, аналізу та візуалізації інформації з відкритих джерел. Такі фреймворки забезпечують стандартизацію процесів відкритої розвідки, підвищуючи ефективність, відтворюваність та масштабованість аналітичної діяльності. Завдяки модульному підходу, вони сприяють інтеграції широкого спектра інструментів, джерел даних та аналітичних засобів у єдине функціональне середовище, що дає змогу гнучко адаптувати OSINT-процеси до конкретних завдань, контекстів і ресурсних обмежень.

Наведемо найбільш відомі приклади фреймворки OSINT-інструментів:

1. **OSINT Framework** (*https://osintframework.com*) – найбільший фреймворк OSINT-інструментів, максимально простий та зручний інтерфейс. Всі інструменти структуровані на підрозділи, відповідно до їхнього призначення. OSINT Framework орієнтований на збір інформації з безкоштовних інструментів або ресурсів. Мета – допомогти дослідникам знайти безкоштовні OSINT-ресурси. Деякі з включених сайтів можуть вимагати реєстрації або пропонувати більше даних за підписку, але дослідник має можливість отримати принаймні частину доступної інформації безкоштовно.



2. **AsINT Collection** (*https://start.me/p/b5Aow7/asint_collection*) – створений на базі порталу start.me репозитарій OSINT інструментів та призначений для збирання, обробки та візуалізації інформації з відкритих джерел. Його основна мета – автоматизація рутинних етапів розвідки, надання дослідникам швидкого доступу до релевантних інструментів та платформ, необхідних для аналізу об'єктів дослідження, таких як домени, IP-адреси, соціальні профілі, e-mail, телефони тощо.



Приклад практичного застосування:

Сценарій: розслідування щодо підозрілої кампанії з дезінформації.

OSINT Collection дозволяє:

- *зібрати акаунти, пов'язані зі схожою тематикою;*
- *знайти спільні email або хешовані імена в акаунтах;*
- *виявити спільні IP-адреси, зв'язки через інфраструктуру або контактні дані;*
- *побудувати схему взаємозв'язків.*

10. Які ризики пов'язані з використанням автоматизованих ботів у відкритій розвідці?
11. Які типи інформації можна отримати з WHOIS-запитів і як вони допомагають в атрибуції доменів?
12. Як працюють веб-архіви (наприклад, Wayback Machine) і які обмеження слід враховувати при їх використанні?
13. У чому полягає роль пошукових операторів у точному формулюванні запитів?
14. Які переваги та ризики використання мобільних застосунків для OSINT-розвідки?
15. Як Telegram-боти можуть автоматизувати процес збору відкритої інформації?
16. Які елементи слід враховувати при оцінці надійності інструменту або сервісу?
17. Як забезпечити анонімність при використанні OSINT-інструментів у відкритому середовищі?
18. Які етичні принципи слід дотримуватися при роботі з персональними даними у відкритих джерелах?
19. Як поєднання різних інструментів дозволяє виявляти приховані зв'язки між об'єктами дослідження?
20. Які навички потрібні для ефективної навігації між фреймворками, сервісами та ботами в OSINT-практиці?

РОЗДІЛ 6

МЕТАДАНІ У ЦИФРОВІЙ АНАЛІТИЦІ ВІДКРИТИХ ДЖЕРЕЛ

Станіслав САМОЙЛОВ

У цифрову епоху, коли дедалі більша частина суспільної, економічної та злочинної активності переміщується в онлайн-середовище, вміння аналізувати не лише вміст, а й структурні атрибути даних – стає необхідною компетенцією дослідника. Одним із таких атрибутів є метадані – *«дані про дані»*, які відіграють не останню роль у відкритій розвідці, цифровій криміналістиці та кримінальному аналізі.

Метадані – це структурована інформація, що описує характеристики інших даних. У контексті OSINT-аналітики вони слугують:

- джерелом додаткового контексту (наприклад, час та дата створення файлу);
- індикатором достовірності чи фальсифікації;
- основою для побудови взаємозв'язків між об'єктами.

Прості приклади метаданих включають: *дату зйомки фото, координати місця, де воно зроблено, інформацію про пристрій, яким воно створене, IP-адресу публікації, ідентифікатор облікового запису* тощо.

Цікавий факт, якщо ви думаєте, що метадані прийшли разом із загальною цифровізацією, то ви не зовсім праві. Перші стандартизовані метадані використовувалися в бібліотеках задовго до появи комп'ютерів – це були бібліографічні картки.

У цифровій аналітиці відкритих джерел застосовуються такі типи метаданих:

- *технічні* – описують характеристики файлів (формат, розмір, версія ПЗ, GPS- координати, EXIF-дані);
- *контентні* – визначають тематику або зміст (ключові слова, заголовки, хештеги);
- *адміністративні* – містять дані про походження, автора, джерело, ліцензії, права доступу;
- *соціальні* – формуються у соціальних мережах (коментарі, репости, взаємодії);
- *мережеві* – включають інформацію про цифрові маршрути (IP-адреси, заголовки HTTP, адреси DNS);
- *геопросторові* – містять координати, картографічні дані (важливо для фото, супутникових знімків, відео).

Так, *смартфон* зберігає в фото *EXIF-метадані*: *час, місце зйомки, камера*. *Текстовий документ* містить *інформацію про автора, кількість сторінок, дату останнього збереження*. *Аудіофайл* містить теги: *назва композиції, виконавець, жанр*.

Про важливість метаданих може свідчити той факт, що у 2011 році американський журналіст виявив місце дислокації військової бази США в Іраку завдяки EXIF-даним з фото, опублікованого солдатом у Facebook.

Аналіз метаданих можливий у таких цифрових об'єктах:

Об'єкт	Типи доступних метаданих
Зображення	EXIF (дата, час, геолокація, модель пристрою, серійний номер)
Відео	дата зйомки, роздільна здатність, кодек, джерело завантаження
Документи	автор, редактор, дата створення та зміни, версії ПЗ
Веб-сторінки	метатеги, CMS, час публікації, URL-структура, ID користувача
Публікації в соцмережах	ID поста, точна дата, IP-адреса, геотеги, зв'язки між акаунтами

Як використовуються метадані в OSINT:

Сфера OSINT	Як використовуються метадані
Розслідування подій	*встановлення дати, часу, місця зйомки*
Виявлення авторства	*ідентифікація автора за властивостями файлу*
Контроль дезінформації	*перевірка джерел походження матеріалів*
Аналіз документів	*виявлення слідів редагування, плагіату, фейків*

Як переглянути та видалити метадані:

- **ПК:** *натиснути на правую клавішу → «Властивості» → «Подробиці»;*
- **macOS:** *виділити файл та натиснути комбінацію клавіш ⌘ + I (Get Info);*
- **он-лайн:** *використовувати онлайн інструменти, про які далі в цьому розділі.*

Видалення метаданих відбувається або в ручну, або за допомогою додаткових онлайн/офлайн інструментів.

На практиці використовують різні інструменти аналізу метаданих у відкритому доступі. Так, платформа **ASPOSE** (*https://products.aspose.app/words/ru/metadata*)

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке метадані і яку роль вони відіграють у цифровій аналітиці?
2. Які основні типи метаданих використовуються в OSINT-дослідженнях?
3. Як метадані допомагають верифікувати джерело цифрового контенту?
4. Які приклади метаданих можна знайти у фотографіях, відео та текстових файлах?
5. Які платформи соціальних медіа автоматично видаляють метадані при завантаженні контенту?
6. Як EXIF-дані можуть бути використані для визначення місця, часу та пристрою зйомки?
7. Чому метадані вважаються прихованим джерелом інформації у SOCMINT?
8. Які інструменти дозволяють вилучати метадані з цифрових файлів?
9. Як метадані можуть допомогти в побудові часової лінії подій?
10. Які ризики виникають при публікації контенту з незахищеними метаданими?
11. Як метадані можуть вказувати на авторство або першоджерело цифрового матеріалу?
12. Які елементи метаданих є найбільш корисними для аналізу поведінки користувача?
13. Як метадані можуть бути використані для виявлення зв'язків між об'єктами розслідування?
14. Які юридичні та етичні обмеження слід враховувати при роботі з метаданими?
15. Як метадані можуть бути змінені або підроблені — і як це впливає на достовірність аналізу?
16. Які формати файлів найчастіше містять багаті метадані?
17. Як метадані можуть бути інтегровані в загальну OSINT-стратегію?
18. Чому важливо враховувати контекст метаданих при їх інтерпретації?
19. Як метадані можуть допомогти у виявленні цифрових слідів, які не видно на поверхні?
20. Які прикладні сценарії використання метаданих у кібербезпеці, розслідуваннях або журналістиці?

РОЗДІЛ 7

СОЦІАЛЬНІ МЕРЕЖІ

Наталія СВИРИДЮК

СОЦІАЛЬНІ МЕРЕЖІ ЯК СЕРЕДОВИЩЕ OSINT-РОЗВІДКИ

У контексті сучасного цифрового суспільства соціальні мережі відіграють критично важливу роль у формуванні комунікаційних процесів, поширенні інформації, мобілізації спільнот та впливі на суспільні настрої. Вони стали не лише інструментом міжособистісного спілкування, а й платформою для організації соціальних, політичних і комерційних ініціатив.

Для фахівців у сфері OSINT соціальні мережі є надзвичайно цінним джерелом

відкритої інформації. Вони дозволяють здійснювати моніторинг поведінкових патернів, інформаційних потоків, мережевих зв'язків та цифрової активності об'єктів дослідження. Цей тип розвідки має окрему назву – SOCMINT (Social Media Intelligence), що позначає систематичне дослідження соціальних медіа у контексті безпеки, розслідувань та аналітики.

З огляду на стрімку еволюцію цифрових платформ, соціальні мережі вже давно вийшли за межі класичних форматів. Сучасний ландшафт включає банківські сервіси, платформи знайомств, ігрові екосистеми, бізнес-інструменти, блоги, оглядові сайти, стримінгові сервіси та дискусійні майданчики. Це динамічне середовище, яке постійно змінюється, і тому потребує системного моніторингу з боку аналітика або слідчого.

Варто зазначити, що доступ до соціальних мереж не означає автоматичного отримання конфіденційної інформації. Натомість дослідник має змогу аналізувати публічний імідж об'єкта, його комунікаційні стратегії, заявлені позиції та соціальні зв'язки. Це дозволяє оцінити характер загроз, розрізнити реальні ризики від демонстративної поведінки, а також виявити потенційні точки впливу.

Соціальні мережі також відіграють роль у пошуку осіб, встановленні контактів, виявленні зв'язків між групами, а в окремих випадках – у вивченні механізмів масової мобілізації. Приклади таких процесів включають політичні кампанії, громадські рухи (наприклад, Black Lives Matter або Арабська весна), а також комерційні активності, що генерують мільярдні обороти.

У межах SOCMINT-розслідувань особливу цінність має здатність встановлювати зв'язки між об'єктами – незалежно від того, чи йдеться про особисті акаунти, корпоративні сторінки, групи або коментарі. Навіть один виявлений зв'язок може стати ключовим елементом у побудові аналітичної картини або доказової бази.

БАЗОВІ ПОЛОЖЕННЯ SOCMINT: ТЕРМІНИ, РИЗИКИ, ТЕХНІЧНІ ОСНОВИ

Перш ніж розпочати роботу з соціальними мережами в контексті OSINT-розслідувань, слідчий має усвідомити дві ключові проблеми. Перша – це захист власної цифрової присутності під час дослідження відкритих джерел. Друга – постійне оновлення знань про те, які платформи використовуються, ким і як. Обидва завдання є складними, оскільки ландшафт соціальних медіа змінюється надзвичайно швидко.

Основи термінології: символи, які відкривають доступ

У соціальних мережах існують умовні позначення, які допомагають структурувати контент і здійснювати пошук:

- **Хештег (#)** – позначає тему або ключове слово. Наприклад: *#osintforgood, #tgif*. Хештеги складаються з одного слова або фрази без пробілів.
- **Собачка (@)** – вказує на конкретний акаунт. Наприклад: *@jimmyfallon, @hetheringtongrp*.

Ці символи стали стандартом на більшості платформ – від X (колишній Twitter) до Instagram, TikTok, Facebook, Reddit. Вони дозволяють швидко знаходити контент, пов'язаний з певною темою або особою.

Джерела знань: що варто читати

Через швидкоплинність змін у соціальних мережах, жоден посібник не може залишатися актуальним надовго. Проте існують фундаментальні джерела, які варто мати під рукою:

- **Michael Bazzell – Open Source Intelligence Techniques (2024)** Регулярно оновлювана книга, яка містить практичні методи пошуку в соцмережах.

спостереження?

18. Як соціальні медіа-платформи можуть бути використані для виявлення ризиків, пов'язаних із людським фактором?
19. Чому важливо розуміти очікування користувачів щодо конфіденційності на різних платформах?
20. Як аналітик може забезпечити етичність і законність своїх дій у процесі SOCMINT-дослідження на прикладі конкретних платформ?

РОЗДІЛ 8

ПОШУК ОСІБ У ЦИФРОВОМУ СЕРЕДОВИЩІ

Карен ІСМАЙЛОВ

Інтернет зберігає величезну кількість інформації про кожного користувача мережею Інтернет – від офіційних контактів до випадкових згадок у коментарях. Знаючи, де шукати, можна знайти людину навіть за мінімальними даними. Цей розділ присвячений практичним методам пошуку інфрмації за електронною поштою, іменем та телефонним номером.

Кожен метод має свої особливості і обмеження, але разом вони створюють потужний інструментарій для OSINT-досліджень.

ІДЕНТИФІКАЦІЯ ЗА ЕЛЕКТРОННИМИ ПОШТОВИМИ АДРЕСАМИ

Електронна пошта залишається одним з найстабільніших ідентифікаторів людини в мережі. На відміну від нікнеймів, які легко змінити, email-адреси часто використовуються роками та прив'язані до десятків сервісів – від соцмереж до онлайн-магазинів. Знаючи електронну пошту людини, можна знайти її профілі, відновити ланцюжок активності або просто встановити контакт.

Пошук електронної адреси особливо корисний, коли потрібно знайти професійні контакти, перевірити автентичність співрозмовника або з'ясувати, чи не використовується певна адреса в підозрілій діяльності. Чому взагалі варто говорити про email у 2025 році, коли всі сидять у месенджерах? Тому що електронна пошта нікуди не зникла і не збирається. Це все ще обов'язковий атрибут реєстрації майже скрізь, основний канал ділової комунікації та єдиний спосіб відновити доступ до акаунтів, якщо щось пішло не так. Email працює скрізь – від банківських додатків до державних порталів. Це той самий універсальний ключ, який відкриває більшість дверей в інтернеті.

До інструментів пошуку можна віднести:

Hunter.io (*https://hunter.io*). Спеціалізований сервіс для пошуку корпоративних email-адрес. Достатньо ввести домен компанії (наприклад, company.com), і Hunter покаже список електронних адрес співробітників, знайдених у відкритих джерелах. Корисно для пошуку контактів PR-менеджерів, керівників або інших фахівців. Безкоштовна версія дозволяє 25 запитів на місяць. Також є функція перевірки формату email – сервіс підкаже, чи існує адреса насправді.

Snov.io (*https://snov.io*). Альтернатива Hunter з додатковими можливостями. Окрім пошуку по доменах, Snov.io може витягувати email з LinkedIn-профілів (через розширення для браузера) та перевіряти валідність адрес. Дозволяє шукати контакти за посадою, географією та іншими параметрами. Безкоштовно – 50 кредитів на місяць.

Google Dorks (*Google Hacking*, *Google Dorking*) *для email*. Пошукові оператори

РОЗДІЛ 9

OSINT ДОСЛІДЖЕННЯ ФОТОЗОБРАЖЕНЬ ТА ВІДЕОКОНТЕНТУ

Дмитро АФОНІН

ФОТОЗОБРАЖЕННЯ ТА ВІДЕОКОНТЕНТ ЯК ОБ'ЄКТИ OSINT-ДОСЛІДЖЕНЬ

Актуальність фотозображень та відеоконтенту в OSINT-дослідженнях. Фотозображення та відеоконтент є фундаментальними об'єктами OSINT-досліджень, оскільки вони становлять візуальні дані, що збираються з відкритих джерел, таких як соціальні медіа, новинні портали та інші онлайн-платформи. Ці об'єкти, будучи частиною відкритої інформації (OSINF), слугують первинною сировиною для OSINT, надаючи візуальні докази, які можуть підтверджувати інші види розвідувальних даних. Вони дозволяють ідентифікувати локації, осіб, об'єкти та дії, забезпечуючи контекст, який не може бути повністю отриманий лише текстовою інформацією. OSINT включає збір та аналіз відео, аудіо та текстових даних з публічних джерел, причому їх аналіз часто базується на алгоритмах машинного навчання та глибоких нейронних мережах.

Актуальність дослідження фотозображень та відеоконтенту в сучасному OSINT невпинно зростає. У сучасному цифровому світі, де злочинність та тероризм адаптувалися до використання соціальних медіа та зашифрованих повідомлень, візуальний контент став незамінним інструментом для правоохоронних органів та розвідувальних служб. Він дозволяє виявляти приховані мережі, відстежувати діяльність та вживати проактивних заходів проти загроз. Візуальний OSINT є критично важливим для підвищення ситуаційної обізнаності в реальному часі під час криз, громадських заворушень або подій, що розгортаються. Наприклад, журналісти активно використовують OSINT для перевірки фактів та проведення розслідувань, зокрема документування воєнних злочинів та викриття корупційних схем, де фото- та відеоматеріали відіграють ключову роль як докази. OSINT, зокрема з соціальних медіа, є потужним інструментом для збору інформації, що охоплює аналіз мультимедійного контенту для отримання уявлень про індивідуальну поведінку та ширші суспільні тенденції.

Проліферація (розповсюдження) цифрових медіа та соціальних мереж не просто додала візуальний контент до OSINT, а трансформувала його, зробивши візуальну розвідку невід'ємною частиною майже всіх інших розвідувальних напрямків. Спочатку OSINT визначався як збір даних з публічних джерел, включаючи текст, відео, зображення та аудіо. Згодом стало очевидним, що соціальні медіа є основним джерелом візуального контенту для OSINT. Це призвело до того, що SOCMINT (розвідка з соціальних мереж) стала визнаним підрозділом OSINT. Водночас, GEOINT (геопросторова розвідка) також активно використовує супутникові знімки та географічні дані, а IMINT (розвідка зображень), в свою чергу, є її підрозділом. Така взаємодія свідчить про те, що зростання обсягів користувацького візуального контенту (фото, відео) у соціальних мережах є рушійною силою для розвитку візуального OSINT. Цей контент часто містить геотеги та інші метадані, що робить його надзвичайно цінним для GEOINT. Таким чином, візуальний контент виступає як наскрізний елемент, що пов'язує різні напрямки OSINT (SOCMINT, GEOINT/IMINT), а не просто є одним із типів даних. Ця інтеграція вимагає від аналітиків ширшого набору навичок, що охоплюють як соціальні медіа, так і геопросторовий аналіз, а також розуміння взаємозв'язків між цими джерелами.

Однак, ця величезна доступність даних є *«палицею з двома кінцями»*. Незважаючи на те, що OSINT вважається юридично та етично прийнятним, оскільки

7. Які інструменти дозволяють перевірити автентичність відео?
8. Як можна визначити місце зйомки за архітектурними елементами на фото?
9. Які методи дозволяють виявити фейкові або змонтовані відео?
10. Як погодні умови на фото можуть допомогти у верифікації події?
11. Які платформи дозволяють здійснювати зворотний пошук відео або кадрів?
12. Як аналіз контексту зображення допомагає у встановленні обставин події?
13. Які етичні обмеження слід враховувати при використанні візуального контенту?
14. Як можна виявити джерело походження відео, якщо воно поширене без авторства?
15. Які ознаки можуть свідчити про постановочний характер відео?
16. Як можна використати геолокаційні сервіси для підтвердження місця зйомки?
17. Які ризики виникають при неправильній інтерпретації візуального контенту?
18. Як відео може бути використане для реконструкції хронології подій?
19. Які платформи соціальних медіа найчастіше використовуються для поширення візуального контенту?
20. Як аналітик OSINT може інтегрувати аналіз зображень і відео у загальну розвідувальну стратегію?

РОЗДІЛ 10

АНАЛІЗ ВІРТУАЛЬНИХ АКТИВІВ З ВИКОРИСТАННЯМ OSINT ІНСТРУМЕНТІВ ТА ОГЛЯДАЧІВ

Євгеній ПАНЧЕНКО

Дослідження навколо природи і особливостей функціонування віртуальних активів все частіше з'являються у науковому дискурсі, починаючи від технічних і технологічних аспектів, їх природи та особливостей функціонування, продовжуючи правовими аспектами регулювання, а також протидії незаконній діяльності, яка здійснюється з їх використанням.

Розглянемо наявні способи та засоби аналізу віртуальних активів з використанням відкритих джерел, зокрема OSINT підходи, що допомагають у базовій аналітиці руху віртуальних активів, встановленні фактів наявності чи відсутності активів на конкретних криптогаманцях, а також ідентифікації певних сутностей, що можуть допомогти у розкритті інформації щодо власників та пов'язаних осіб з конкретними віртуальними активами.

Варто зазначити, що віртуальні активи не являються однорідною категорією та охоплюють низку різних типів активів, що різняться за функціональним призначенням, рівнем ризику та правовим статусом. У сучасній правозастосовній практиці та нормативному регулюванні застосовується кілька моделей класифікації віртуальних активів, які використовуються зокрема у Європейському Союзі, США, Великій Британії, Швейцарії, Сінгапурі та Україні.

Для аналізу віртуальних активів варто зробити відповідну класифікацію:

- *платіжні токени (Payment Tokens) – токени, що функціонують як засіб обміну або платежу*. Найбільш відомими прикладами є **Bitcoin (BTC)** та **Litecoin (LTC)**. Їх правовий статус визначено, зокрема, у керівництві FATF

та настановах FINMA;

- *стабільні монети (Stablecoins) – віртуальні активи, вартість яких забезпечується резервом активів або підтримується алгоритмічно.* Регламент MiCA виокремлює їх у підкатегорії: *«asset-referenced tokens»* (**ART**) та *«electronic money tokens»* (**EMT**);
- *інвестиційні токени (Security Tokens) – цифрові активи, що відображають права на частку власності, прибуток або боргові зобов'язання.* У ЄС вони регулюються в рамках MiFID, у США – згідно з законодавством SEC;
- *утилітарні токени (Utility Tokens) – надають доступ до цифрового продукту або послуги в межах певної екосистеми.* Хоча такі токени часто не вважаються фінансовими інструментами, регулятори (зокрема FCA та FinCEN) акцентують увагу на їх використанні у схемах шахрайства;
- *невзаємозамінні токени (NFT, Non-Fungible Tokens) – унікальні цифрові активи, що підтверджують право власності на об'єкт.* У MiCA зазначено, що NFT загалом не підпадають під дію регламенту;
- *обгорнуті токени (Wrapped Tokens) – похідні токени, що відображають інші активи на альтернативних блокчейнах.* Їх правовий статус розглядається залежно від базового активу;
- *гібридні токени (Hybrid Tokens) – поєднують функції кількох типів (утилітарні, інвестиційні, платіжні).* Вимагають індивідуального правового аналізу;
- *DAO-токени (Governance Tokens) – забезпечують участь в управлінні децентралізованими автономними організаціями.* Часто мають риси security-token залежно від контексту;
- *CeFi Tokens – токени централізованих платформ (BNB, FTT), що можуть використовуватись для доступу до послуг, інвестування або знижок;*
- *електронні грошові токени (E-money Tokens) – прирівнюються до електронних грошей і регулюються як такі відповідно до Директиви про електронні гроші (Directive 2009/110/EC) та PSD.*

Національна класифікація України – Закон України *«Про віртуальні активи»* визначає їх як нематеріальні блага у формі цифрового вираження вартості, що існують в інформаційній системі. Також віртуальні активи визначені як об'єкти цивільно-правових відносини у Цивільному кодексі України, де їх статус зазначено як цифрова річ. У зв'язку з тим, що саме Цивільний кодекс на відміну від профільного закону є чинним, ми зосередимо увагу на найбільш популярних типах віртуальних активів, базуючись на практичних аспектах діяльності підрозділів, що здійснюють розслідування злочинів пов'язаних з віртуальними активами.

АНАЛІЗ ПЛАТІЖНИХ ТОКЕНІВ ТА СТАБІЛЬНИХ МОНЕТ З ВИКОРИСТАННЯМ ВІДКРИТИХ ДЖЕРЕЛ

Цей вибір здійснений з урахуванням популярності використання саме цих типів віртуальних активів у національній екосистемі обігу віртуальних активів, у тому числі у незаконній діяльності. Популярність стабільних токенів підсилюється їх майже винятковим використанням у так званих офлайн обмінниках, які працюють переважно під виглядом обмінних пунктів іноземної валюти і також, доволі часто, здійснюють обмін віртуальних активів у вигляді стабільних токенів, переважно USDT у мережі TRON.

Open-Source Intelligence (OSINT) – це збір, обробка та аналіз інформації з відкритих джерел, що публічно доступна для використання. У контексті розслідувань,

18. Що таке *«Contract Internal Transactions»* в Etherscan і чому вони важливі?
19. Які OSINT-інструменти загального призначення допомагають пов'язати гаманці з соцмережами?
20. Як Telegram-боти типу Whale Alert або Scam Sniffer використовуються в оперативному аналізі?

РОЗДІЛ 11

DARK WEB ТА АНОНІМНІСТЬ В ІНТЕРНЕТІ: ДОСЛІДЖЕННЯ ПРИХОВАНОГО ІНТЕРНЕТУ

Олександр Олександрович КОРИСТІН

Темний веб (**Dark Web**), частина глибинного вебу (**Deep Web**), який складається з декількох даркнет-мереж (наприклад, **Tor**, **I2P** і **Freenet**), надає користувачам можливість приховувати свою особистість під час серфінгу або публікації інформації. Така анонімність полегшує передачу конфіденційних даних для законних цілей, але також забезпечує ідеальне середовище для передачі інформації, товарів і послуг з потенційно незаконними намірами.

За останні 25 років *Всесвітня павутина* (**WWW**) стала найпопулярнішим інструментом, який використовують мільярди користувачів для пошуку новин, розваг, спілкування та інших цілей. На відміну від того, що може подумати пересічний користувач, лише невелика частина Інтернету є легкодоступною. Поверхневий веб (*Surface Web*) – це частина Інтернету, яка збирається та індексується звичайними пошуковими системами загального призначення, такими як Google, Yahoo! або Bing , а потім стає доступною широкому загалу за допомогою типових веб-браузерів, таких як Mozilla Firefox, Google Chrome або Internet Explorer. Однак, подібно до того, як над водою видно лише верхівку айсберга (*рис.1*), тоді як переважна більшість його маси лежить під водою, пошукова система загального призначення здатна індексувати лише невелику частину інформації, доступної в Інтернеті; решта неіндексованого контенту лежить у глибинному вебі (*Deep Web*). Пошук за допомогою популярних пошукових систем, таких як Google і Bing, не зробить вас професійним користувачем Інтернету, оскільки все, що ви бачите на цих сайтах, - це лише частина поверхневого вебу, яка становить лише 4% від усього веб-контенту.

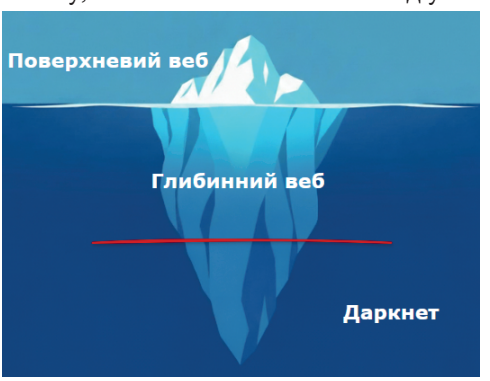


Рисунок 1. Структура Всесвітньої павутини (WWW)

Глибинний веб, також відомий як Прихований або Невидимий веб, загалом складається з інформації, яку неможливо отримати за допомогою запиту до звичайної пошукової системи загального призначення. Контент, присутній у

РОЗДІЛ 12

РЕЄСТРИ ДЕРЖАВНИХ ОРГАНІВ

Юрій КАРДАШЕВСЬКИЙ

Реєстри державних органів є систематизованими джерелами структурованої інформації, що мають критичне значення для OSINT-аналітики. Вони містять дані про юридичних осіб, фізичних осіб-підприємців, нерухомість, судові рішення, транспортні засоби, ліцензії, тендери, санкції, митні операції, фінансову звітність та інші аспекти публічного життя.

Доступ до реєстрів може бути відкритим, обмеженим або платним, а їхнє використання регулюється законодавством про захист персональних даних, публічну інформацію та доступ до відкритих даних. Ефективна робота з реєстрами передбачає знання їхньої структури, логіки пошуку, типів ідентифікаторів (ЄДРПОУ, ІПН, VIN, кадастровий номер тощо), а також вміння поєднувати дані з різних джерел для побудови аналітичної картини.

Реєстри дозволяють верифікувати факти, виявляти зв'язки, оцінювати ризики та формувати доказову базу в OSINT-розслідуваннях.

Єдині та державні реєстри створені й функціонують відповідно до законодавства України (законів України, актів Кабінету Міністрів України, відомчих нормативно-правових актів, а також інших документів правового характеру).

> *Вважається, що, якщо не доведено інше, інформація, наведена в державному реєстрі, є правильною та правдивою і не підлягає доказуванню.*

В Україні відбувається активне формування державних реєстрів у різних галузях життя держави.

ПЕРЕЛІК НАЙПОПУЛЯРНІШИХ ДЕРЖАВНИХ РЕЄСТРІВ УКРАЇНИ:

Єдиний державний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань – система розкриття інформації про юридичних осіб та підприємців;

Єдиний державний реєстр судових рішень – база даних судових рішень України;

Єдиний державний реєстр нормативних актів – база даних для об'єднання нормативних актів, що перебувають у державному обліку;

Державний реєстр фізичних осіб – автоматизований банк даних, створений для забезпечення єдиного державного обліку фізичних осіб;

Єдиний державний реєстр виборців і Єдина електронна інформаційна система «Вибори» – Державний реєстр виборців України.

Пошук за державними реєстрами можна здійснити на Порталі відкритих даних за посиланням *https://data.gov.ua,* який має наступні категорії пошуку:

- *Держава:* все що стосується державного управління та питань загально-державного характеру.
- *Державні доходи і видатки:* закупівлі, витрати, бюджетні показники.
- *Економіка та бізнес:* все про компанії, питання пов'язані з веденням господарської діяльності.
- *Енергетика:* тарифи, видобування, споживання, імпорт/експорт енергоносіїв.
- *Інфраструктура і транспорт:* транспорті засоби, маршрути, перевезення, ремонт та будівництво шляхів.
- *Навколишнє середовище:* екологія, тваринний/рослинний світ, свердловини,

водні ресурси, якість повітря/води, клімат тощо.

- *Освіта, культура, спорт:* навчальні заклади, освітні програми, культурні/історичні пам'ятки, інфо-матеріали (виробництво/розповсюдження), кіно-,аудіо-індустрія, активний відпочинок, спортивна діяльність.
- *Охорона здоров'я:* захворювання, лікарські засоби, лікарні, формуляри.
- *Регіональний розвиток:* територіальні громади, комунальна власність, місцевий розвиток.
- *Суспільство:* громадянське суспільство, соціальні стандарти та захист, пільги.
- *Фінанси:* державні гарантії, звіти, бюджетні програми.
- *Юстиція та судочинство:* нормативно-правові засади діяльності держави, суди та судочинство, правоохоронна діяльність.

Інформаційно-пошукова система **PROZORRO** (*www.prozorro.gov.ua*) забезпечує прозорість, відкритість та контроль за проведенням публічних закупівель в Україні, тобто в ній зберігається вся інформацію про закупівлі. Комерційні майданчики – надають доступ до системи (наприклад: *Zakupki.Prom.ua*, *E-Tender*, *SmartTender* тощо).

ПЕРЕЛІК ІСНУЮЧИХ ПУБЛІЧНИХ ЕЛЕКТРОННИХ РЕЄСТРІВ

№ п/п	Назва реєстру	Держатель публічного електронного реєстру	Короткий опис	Електронне посилання (за наявності)
1	Державний реєстр актів цивільного стану громадян	Міністерство юстиції України	Державний реєстр актів цивільного стану громадян - це державна електронна інформаційна система, яка містить відомості про акти цивільного стану, зміни, що вносяться до актових записів цивільного стану, їх поновлення та припинення їхньої дії та відомості про видачу свідоцтв про державну реєстрацію актів цивільного стану і про видачу витягів з нього.	https://regdracs.minjust.gov.ua
2	Державний реєстр атестованих судових експертів	Міністерство юстиції України	Державний реєстр атестованих судових експертів - це електронна база даних, що ведеться таконтролюється Міністерством Юстиції України з метою створення інформаційного фонду про осіб, які отримали в порядку, передбаченому Законом України «Про судову експертизу» кваліфікацію судового експерта.	https://rase.minjust.gov.ua/
3	Державний реєстр іпотек	Міністерство юстиції України	Держа́вний реє́стр іпоте́к — єдина комп'ютерна база даних про обтяження і зміну умов обтяження нерухомого майна іпотекою, відступлення прав за іпотечним договором, передачу, анулювання, видачу дубліката заставної та видачу нової заставної.	
4	Державний реєстр обтяжень рухомого майна	Міністерство юстиції України	Державний реєстр обтяжень рухомого майна (ДРОРМ) - це єдина комп'ютеризована база даних, що містить записи про обтяження рухомого майна та звернення стягнень на нього. Іншими словами, це система, де фіксуються всі юридичні обмеження прав власника рухомого майна, а також інформація про те, як ці обмеження можуть впливати на розпорядження цим майном	https://orm.minjust.gov.ua/
5	Державний реєстр речових прав на нерухоме майно	Міністерство юстиції України	Державний реєстр речових прав на нерухоме майно (ДРРП) – це єдина державна інформаційна система в Україні, яка містить відомості про права на нерухомість, їх обтяження, а також про об'єкти та суб'єктів цих прав. Іншими словами, це база даних, де зберігається інформація про власників нерухомості, їх права на неї, а також будь-які обмеження цих прав (наприклад, застава, оренда)	https://rrp.minjust.gov.ua/
6	Електронний реєстр апостилів	Міністерство юстиції України	Електронний реєстр апостилів – це онлайн-база даних, яка містить інформацію про апостилі, видані в Україні. За допомогою цього реєстру можна перевірити достовірність апостиля, а також отримати інформацію про документи, на які він був проставлений	http://era.minjust.gov.ua/
7	Електронний реєстр нотаріальних дій	Міністерство юстиції України	Електронний реєстр нотаріальних дій – це система, яка забезпечує електронний облік та зберігання інформації про вчинені нотаріальні дії. Він є частиною системи «Е-нотаріат» і дозволяє нотаріусам вносити записи про вчинені дії, а також отримувати доступ до необхідної інформації з інших реєстрів та баз даних	https://enot.minjust.gov.ua/
8	Єдиний державний реєстр нормативно-правових актів	Міністерство юстиції України	Єдиний державний реєстр нормативно-правових актів (ЄДРНА) є державною інформаційно-комунікаційною системою, яка ведеться Міністерством юстиції України. До Реєстру включаються чинні, опубліковані та неопубліковані нормативно-правові акти, включаючи закони України, постанови Верховної Ради, укази та розпорядження Президента, декрети, постанови та розпорядження Кабінету Міністрів, а також акти міністерств та інших центральних органів виконавчої влади, зареєстровані в Мін'юсті, та міжнародні договори України. Метою створення ЄДРНА є забезпечення доступу до актуальної та достовірної інформації про нормативно-правові акти, що діють в Україні. Реєстр є важливим інструментом для забезпечення прозорості та відкритості правової системи.	https://www.reestrnpa.gov.ua/
9	Єдиний державний реєстр осіб, щодо яких застосовано положення Закону України «Про очищення влади»	Міністерство юстиції України	Єдиний державний реєстр осіб, щодо яких застосовано положення Закону України «Про очищення влади», – це електронна база даних, що містить інформацію про осіб, на яких поширюється дія заборон, передбачених Законом України «Про очищення влади». Реєстр ведеться Міністерством юстиції України.	https://lustration.minjust.gov.ua/
10	Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань	Міністерство юстиції України	Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань — публічний реєстр юридичних осіб України, що виконує роль державного контролю та захисту прав юридичних осіб, громадських формувань та підприємців України, а також захисту прав третіх осіб у правовідносинах з ними.	https://usr.minjust.gov.ua/
11	Єдиний реєстр арбітражних керуючих України	Міністерство юстиції України	Єдиний реєстр арбітражних керуючих України - це електронна база даних, яка містить інформацію про осіб, що мають свідоцтво про право на здійснення діяльності арбітражного керуючого. Цей реєстр ведеться державним органом з питань банкрутства у складі Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань. Арбітражні керуючі, яких також називають розпорядниками майна, керуючими санацією або ліквідаторами, призначаються судом для управління справами про банкрутство.	https://asbn.minjust.gov.ua/

15. Які інструменти дозволяють здійснювати пошук по кількох реєстрах одночасно?
16. Як можна виявити зв'язки між особами через перехресний аналіз реєстрів?
17. Які реєстри мають API-доступ для автоматизованої аналітики?
18. Як перевірити достовірність даних, отриманих із реєстрів?
19. Які ризики виникають при неправильному трактуванні інформації з реєстрів?
20. Як інтеграція реєстрових даних покращує якість OSINT-розслідувань?

РОЗДІЛ 13

OSINT-ЕКОСИСТЕМА СПЕЦІАЛІЗОВАНОГО ФРЕЙМВОРКУ: Maltego, Artellence, Clearview, Hunchly, Lampyre

Ярослав ЛІХОВІЦЬКИЙ

Требо відмітити, що для здійснення професійного та на постійній основі OSINT використання відкритих інструментів не призведе до бажаного результату, так як останні часто перестають працювати (оновлюватись), забороняються законами, та є такими, що не зовсім зручні, обмежені функціонально тощо. Тому зручніше використовувати платні (пробний період безоплатний) *універсальні OSINT-інструменти для соціальних мереж:* **Maltego**, **i2 Analyst's Notebook**, **Artellence**, **Clearview**, **Hunchly**, **Lampyre**, які відіграють ключову роль у процесі цифрової трансформації правоохоронної діяльності та розвідувального аналізу і демонструють сучасні підходи до збору, структурування та візуалізації оперативно значущої інформації.

Maltego забезпечує глибокий графовий аналіз взаємозв'язків між об'єктами, дозволяючи ефективно виявляти цифрові й соціальні мережі в кримінальних структурах.

i2 Analyst's Notebook використовується для стратегічного аналізу, тимчасової та просторової візуалізації складних розслідувань і підтримки ухвалення управлінських рішень.

Artellence реалізує функції розпізнавання облич у відеопотоці, що критично важливо для оперативного виявлення осіб, причетних до правопорушень.

Clearview AI надає доступ до великої бази відкритих зображень із соцмереж, підтримуючи глибоку біометричну ідентифікацію в режимі OSINT.

Hunchly виконує роль цифрового нотаріуса – автоматично зберігаючи, хешуючи та документуючи кожен крок аналітика під час розслідувань у вебсередовищі.

Lampyre є гнучким аналітичним середовищем для комплексного OSINT-аналізу, побудови графів зв'язків і роботи з великими масивами даних з відкритих і напіввідкритих джерел.

У контексті розвитку цифрової розвідки з відкритих джерел, фреймворк *Maltego* виступає як один із найпотужніших інструментів для візуального аналізу даних, виявлення зв'язків та побудови аналітичних графів взаємодії між об'єктами дослідження. Його функціональні можливості забезпечують інтеграцію з великою кількістю зовнішніх джерел, що формує повноцінну OSINT-екосистему, орієнтовану на глибоке вивчення цифрових слідів суб'єктів у відкритих, напіввідкритих і комерційних базах даних.

«У світі відкритих джерел швидкість мислення визначається не людиною, а алгоритмом, який вона створила»

*- Авторська формул*а

У XXI сторіччі розвідка з відкритих джерел перестала бути лише пошуком фактів. Вона стала симбіозом алгоритмів, мовних моделей, коду і критичного мислення. Ми більше не просто шукаємо – ми моделюємо, прогнозуємо, автоматизуємо. І саме тому ця частина присвячена тому, що ще вчора здавалося футуризмом, а сьогодні – вже інструмент у руках аналітика.

Python став універсальною мовою OSINT-дослідника. Його бібліотеки дозволяють не лише збирати дані, а й очищати, структурувати, візуалізувати, будувати графи зв'язків, аналізувати поведінкові патерни. А з появою великих мовних моделей (LLM – Large Language Models) ми отримали новий рівень – можливість працювати з текстом як з даними, автоматизувати аналітичні сценарії, створювати запити (промпти), що не просто шукають, а мислять.

У розділах цієї частини ми розглядаємо, як безкодове програмування та промпт-інжиніринг відкривають двері до OSINT навіть для тих, хто не є програмістом. Як мовні моделі інтегруються в розслідування, допомагаючи аналізувати масиви текстів, відео, цифрових слідів. Як базові скрипти на Python стають основою для автоматизованих перевірок, а складні сценарії – для побудови фінансово-медійних дашбордів.

Це не просто технічна частина. Це – про нову епоху аналітики, де штучний інтелект не замінює людину, а підсилює її здатність бачити глибше, швидше, точніше. Це про те, як OSINT стає не лише інструментом, а й середовищем, у якому мислення програмується, а правда – верифікується алгоритмічно.

ШТУЧНИЙ ІНТЕЛЕКТ ТА PYTHON В OSINT

ЧАСТИНА III

РОЗДІЛ 14

ПРОМПТ ІНЖИНІРИНГ НА ОСНОВІ БЕЗКОДОВОГО ПРОГРАМУВАННЯ

Дмитро ЛАНДЕ
Leonard STRASHNOY

У застосуванні *великих мовних моделей (LLM)* для аналізу та обробки відкритих даних у межах OSINT-методології ключову роль відіграє якість формулювання запитів – створення структурованих, контекстно релевантних і лінгвістично точних промптів. Незважаючи на високу потужність мовних моделей, ефективність їхніх відповідей значною мірою визначається точністю та адекватністю вхідного запиту. У цьому контексті навички побудови ефективних запитів набувають статусу критично важливого елементу професійної компетентності аналітика.

Процес формулювання запиту виходить за межі технічної операції і розглядається як форма інтелектуальної взаємодії між користувачем і моделлю. Він вимагає не лише глибокого розуміння поставленого завдання та очікуваних результатів, а й знання функціональних можливостей мовної моделі, а також уміння адаптувати подання інформації відповідно до її алгоритмічного сприйняття.

Дослідження останніх років демонструють, що від способу подання запиту часто залежить не лише швидкість отримання результату, а й його аналітична цінність.

Ефективність запиту до великої мовної моделі значною мірою визначається низкою ключових характеристик, що безпосередньо впливають на якість отриманої відповіді. Насамперед, важливою умовою є наявність чітко окресленої цілі. Конкретність і однозначність запиту істотно полегшують інтерпретацію завдання моделлю. Замість загального формулювання на кшталт *«Опиши цей текст»*, значно ефективнішими є інструкції типу *«Виділи всі згадані персоналії»*, *«Здійсни переклад на англійську мову»* або *«Сформулюй резюме подій, описаних у тексті»*. Таке уточнення дозволяє моделі зменшити когнітивну невизначеність і пришвидшує процес генерації релевантної відповіді.

Іншою принциповою характеристикою успішного промпту є його контекстуалізація – включення у запит додаткової інформації про умови, середовище або часові рамки, що визначають аналітичну ситуацію. Зокрема, при роботі з політичними, соціальними чи економічними повідомленнями контекст відіграє вирішальну роль. *Наприклад*, формулювання *«Проаналізуй цей допис у Telegram з урахуванням політичної ситуації в Україні на початку 2025 року»* задає не лише завдання, а й уточнює аналітичну перспективу, в якій очікується відповідь. Це сприяє підвищенню релевантності аналізу й уникненню поверхового трактування змісту.

Значного покращення якості результатів можна досягти шляхом використання *техніки few-shot prompting*, яка передбачає надання моделей одного або кількох прикладів бажаного формату відповіді. Такий підхід дозволяє моделі адаптувати стиль і структуру результату до очікувань користувача, що особливо важливо під час обробки структурованих даних, здійснення класифікації або тематичного узагальнення великих текстових корпусів.

Також важливо вказувати очікуваний формат результату. Якщо відповідь моделі має інтегруватися в подальші етапи обробки або вбудовуватись у інформаційні системи, доцільно заздалегідь визначити форму її подання: *JSON, табличне подання, маркований список чи суцільний текст*. Чіткість формату не лише підвищує організованість відповіді, а й полегшує її використання в

автоматизованих аналітичних процесах.

Для аналітиків, які регулярно працюють з великими обсягами текстових або інформаційних даних, рекомендовано створювати стандартизовані шаблони запитів, орієнтовані на типові завдання. Це можуть бути шаблони для класифікації тем, виявлення ознак маніпуляції або дезінформації, ідентифікації ключових суб'єктів, аналізу емоційної тональності або побудови хронологічних послідовностей. Застосування шаблонів забезпечує послідовність взаємодії з LLM, знижує варіативність результатів і скорочує часові витрати на підготовку запитів.

Таким чином, розробка промптів для великих мовних моделей є складовою аналітичної компетентності, що має вагоме значення в контексті роботи з відкритими даними. Ця діяльність виходить за межі суто технічної операції й постає як елемент професійної культури сучасного аналітика, подібно до навичок роботи з кодом, API чи графовими структурами.

КОНЦЕПЦІЯ БЕЗКОДОВОГО ПРОГРАМУВАННЯ

Традиційно розробка програмного забезпечення передбачала ручне створення алгоритмів, написання коду та проєктування структур баз даних. Однак із розвитком систем штучного інтелекту ці завдання дедалі частіше автоматизуються та передаються на виконання інтелектуальним агентам. Відбувається трансформація інтерфейсу взаємодії з даними – від класичного програмування до комунікації природною мовою. У цьому новому середовищі ключовим інструментом управління процесами стають промпти – текстові інструкції, які визначають логіку функціонування мовних моделей і їхню поведінку під час обробки інформації.

Зміни у способах взаємодії з даними та інтелектуальними системами мають певну концептуальну спорідненість з ідеями *Стівена Вольфрама*, викладеними в його праці *«A New Kind of Science»*. Вольфрам запропонував оригінальну наукову парадигму, згідно з якою складні природні явища – такі як дифузія або генерація візерунків – можуть бути результатом дії простих обчислювальних правил, реалізованих у формі клітинних автоматів. Його підхід продемонстрував, що навіть елементарні механізми здатні породжувати високий рівень складності без потреби в класичних математичних моделях.

Незважаючи на те, що ця концепція викликала численні наукові дискусії, її принципова ідея набуває нового значення в епоху широкого впровадження великих мовних моделей (LLM). Подібно до клітинних автоматів, LLM демонструють, що системи з відносно простою структурою взаємодії – зокрема через текстові інструкції природною мовою – здатні ефективно вирішувати завдання високої складності. Це включає операції, які традиційно потребували детального програмування, алгоритмічного моделювання або значних ресурсів для обробки інформації.

У рамках OSINT, де аналітики постійно стикаються з неструктурованими, багатошаровими даними, LLM стають справжньою революцією. На відміну від традиційних інструментів, які потребують жорстко заданих правил або запитів, моделі такого типу адаптуються до контексту, який задається через промпти. Це дозволяє аналітикам формулювати задачі природною мовою, замість написання складних SQL-запитів чи регулярних виразів. *Наприклад*, замість кількох годин на побудову запиту до бази даних, достатньо запитати модель: *«Які найбільш значущі кореляції в цих даних?»* – і отримати результат, готовий до подальшого використання.

Цей механізм нагадує еволюцію від жорстких кодових конструкцій до гнучких, контекстуальних інтерфейсів, де *людина стає не оператором інструменту, а архітектором стратегії*. Проте, як і у випадку з клітинними автоматами, цей підхід не є універсальним. Його ефективність залежить від якості вхідних

26. Як безкодові платформи можуть використовувати блок-схеми?
27. Як безкодове програмування пов'язане з концепцією програмування через приклади (PBE)?
28. Як безкодове програмування забезпечує стандартизацію аналітичних процесів?
29. Як безкодове програмування впливає на масштабованість аналітичних задач?
30. Як безкодове програмування впливає на ефективність аналізу парламентських документів?

РОЗДІЛ 15

ВИКОРИСТАННЯ LLM&PYTHON В OSINT РОЗСЛІДУВАННЯХ

Олексій БАРАНОВСЬКИЙ

YOLOV8 ДЛЯ РОЗПІЗНАВАННЯ ОБ'ЄКТІВ

У цьому розділі ми ознайомимося з потужним інструментом комп`ютерного зору – **YOLOv8**. Ви навчитеся використовувати його для аналізу зображень та отримання практичних результатів у своїх дослідженнях.

Що таке YOLOv8?

YOLOv8 (You Only Look Once, версія 8) – це сучасна модель штучного інтелекту, призначена для завдань комп'ютерного зору. Її головна функція – знаходити та класифікувати різні об'єкти на зображеннях і у відеопотоці. Завдяки високій швидкості та точності, *YOLOv8* є одним зі стандартів у галузі.

Ключові можливості

Модель має широкий спектр застосувань. Основні можливості включають:

- *розпізнавання об'єктів:* YOLOv8 може ідентифікувати людей, транспортні засоби (автомобілі, танки), елементи інфраструктури (будівлі) та багато інших типів об'єктів;
- *детектування кількох об'єктів:* модель здатна одночасно знаходити та розпізнавати десятки різних об'єктів на одному зображенні чи кадрі відео;
- *гнучкість у використанні:* ви можете працювати з YOLOv8 локально, інтегруючи її у свої програми за допомогою бібліотеки для Python, або ж надсилати запити до хмарного сервісу через API.

***Практичний приклад:** Аналіз фото із соціальних мереж*

Розглянемо базове завдання: ви завантажили фотографію із соціальної мережі та хочете автоматично розпізнати, що на ній зображено.

Завдання: Проаналізувати зображення та ідентифікувати на ньому ключові об'єкти.

Кроки виконання (локальний запуск через Python):

1. *Встановіть необхідне середовище:* переконайтеся, що у вас встановлено Python та бібліотеку `ultralytics`.
2. *Підготуйте скрипт:* створіть простий Python-скрипт для завантаження моделі та обробки зображення.

3. *Запустіть розпізнавання:* передайте моделі шлях до вашого зображення.

Приклад коду:

```
from ultralytics import YOLO

# Завантаження попередньо навченої моделі
model = YOLO('yolov8n.pt')

# Запуск розпізнавання на вашому зображенні
results = model('path/to/your/image.jpg')

# Збереження результату
results[0].save(filename='result.jpg')
```

Очікуваний результат

Після обробки ви отримаєте копію вашого зображення, на якому виявлені об'єкти будуть обведені прямокутниками (*bounding boxes*). Кожен прямокутник буде підписано назвою класу об'єкта (*наприклад*, *«танк»*, *«солдат»*, *«будівля»*) та відсотком впевненості моделі.

Важливі примітки

- *Ліцензія:* YOLOv8 поширюється за відкритою open-source ліцензією, що дозволяє використовувати її безкоштовно.
- *Апаратні вимоги:* для швидкої обробки зображень та відео, особливо у великій кількості, рекомендується використовувати комп'ютер з потужною відеокартою (GPU). Без неї аналіз може зайняти значно більше часу.
- *Дисклеймер:* Інструменти командного рядка та програмні інтерфейси можуть змінюватися з виходом нових версій. Слідкуйте за офіційною документацією. У майбутньому може з'явитися наступна версія, наприклад YOLOv9, з новими можливостями та змінами в синтаксисі.

INVID – ПЛАГІН ДЛЯ ВЕРИФІКАЦІЇ ФОТО ТА ВІДЕО

У цьому розділі ми розглянемо *InVID Verification Plugin* – незамінний інструмент для кожного, хто працює з візуальним контентом і прагне перевірити його автентичність.

Що таке InVID Verification Plugin?

InVID Verification Plugin – це розширення (плагін) для веб-браузера, спеціально створене для швидкої та ефективної перевірки фотографій і відео. Його головна мета – допомогти вам виявити маніпуляції та визначити, чи є візуальний контент оригінальним.

Ключові можливості

Плагін надає набір потужних інструментів, зібраних в одному місці:

- *аналіз відео:* автоматичне розбиття відео на ключові кадри (thumbnails), що дозволяє детально проаналізувати його вміст;
- *зворотний пошук зображень:* швидкий пошук вибраних кадрів або фотографій у різних пошукових системах, як-от Google Images або TinEye; це допомагає знайти першоджерело зображення;
- *аналіз метаданих:* можливість отримувати метадані файлу (дату створення, модель камери тощо), хоча ця інформація часто видаляється соціальними мережами.

Посилене завдання

Ціль завдання: Навчитися аналізувати великі багатомовні набори даних.

Покрокові дії:

1. *Завантажити великий набір (100+ повідомлень).*
2. *Попросити класифікувати повідомлення за темами («новини», «особиста думка», «реклама»).*
3. *Виділити дублікати та повтори.*
4. *Скласти зведення:* кількість повідомлень у кожній темі.

Очікуваний результат: Класифікований набір повідомлень і статистика по темах.

Питання для дискусії:

- Які ризики у класифікації великих наборів даних?
- Чи можна довіряти автоматичному видаленню дублікатів?

РОЗДІЛ 16

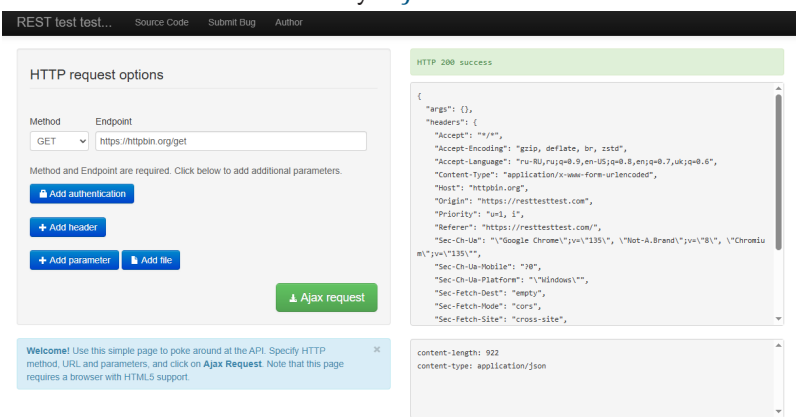
БАЗОВИЙ OSINT-ІНСТРУМЕНТАРІЙ В PYTHON

Олександр Олександрович КОРИСТІН

ОБРОБКА HTTP-ЗАПИТІВ ТА РОБОТА З API

Коли ви відкриваєте веб-сторінку в браузері, відбувається запит до сервера. У відповідь на запит сервер повертає статус, заголовки і тіло відповіді (*наприклад*, html-код веб-сторінки, деякі дані у форматі CSV, JSON або XML).

Для наглядності процесів відкриваємо *https://resttesttest.com,* копіюємо туди якесь посилання і натискаємо кнопку *«AJAX-запит»*.



OSINT часто потребує автоматизації збору даних з веб-сторінок або різних *API (Application Programming Interface – інтерфейс прикладного програмування)*. І основна навичка, необхідна для цього, - написання коду для надсилання запитів до веб-серверів та обробки відповідей.

API – це технологія, яка дозволяє взаємодіяти з додатком, надсилаючи запити на сервер. *Наприклад*, *API Github* дозволяє отримувати дані про користувачів Github, а також вносити зміни до репозиторіїв тощо.

Для цього ми будемо використовувати запити до модулів (*https://pypi.org/project/requests/*).

Встановіть модуль requests: pip install requests

```
!pip install requests

Requirement already satisfied: requests in /usr/local/lib/python3.11/dist-packages (2.32.3)
Requirement already satisfied: charset-normalizer<4,>=2 in /usr/local/lib/python3.11/dist-packages (from requests) (3.4.1)
Requirement already satisfied: idna<4,>=2.5 in /usr/local/lib/python3.11/dist-packages (from requests) (3.10)
Requirement already satisfied: urllib3<3,>=1.21.1 in /usr/local/lib/python3.11/dist-packages (from requests) (2.3.0)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.11/dist-packages (from requests) (2025.1.31)
```

Запустіть *api_request.py*:

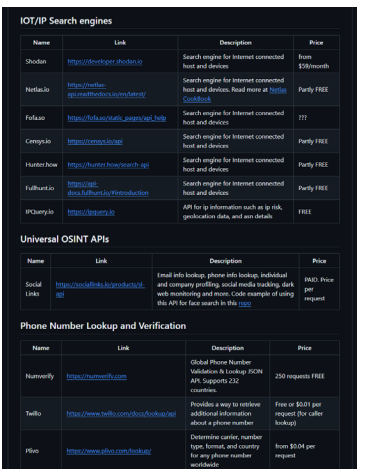
```
import requests

url = "https://api.github.com/search/users?q=javascript"

try:
    response = requests.get(url)

    response.raise_for_status()

    print(response.json())

except requests.exceptions.RequestException as e:
    print(f"Помилка запиту: {e}")

{'total_count': 189653, 'incomplete_results': False, 'items': [{'login': 'javascript', 'id': 48139711, 'node_id': 'MDEyOk9yZ2FuaXphdGlvbjQ4MTM5NzEx',
```

```
# Додайте модуль requests до файлу скрипта за допомогою команди import:
import requests

# Зробіть запит до API:
response =requests.get("https://api.github.com/search/
users?q=javascript")

# Виведіть результат у форматі JSON (JavaScript Object Notation):
print(response.json())
```

Існує величезна кількість API, як платних, так і безкоштовних, які надають корисні дані для OSINT. *Наприклад:*

- *інформація про номери телефонів, адреси та поштові індекси;*
- *інформація про компанії;*
- *інформація про домени та IP-адреси;*
- *інформація про криптогаманці та транзакції;*
- *інформація про користувачів різних соціальних мереж.*

Список понад сотні корисних OSINT API можна знайти в цьому репозиторії на Github: *https://github.com/cipher387/API-s-for-OSINT*



Не обов'язково писати окремий Python-скрипт для тестування різних API. Краще скористатися спеціальними онлайн-сервісами, які можуть імітувати різні типи запитів і методів авторизації.
Наприклад, reqbin.com або *REST API Tester*.

РОЗДІЛ 17

OSINT ІНСТРУМЕНТИ НА ОСНОВІ PYTHON: СКЛАДНІ СЦЕНАРІЇ АНАЛІТИКИ

Олександр ШУКЛІН

Серед всього різноманіття мов програмування Python став програмною реалізацією для багатьох дослідників у сфері OSINT, завдяки своїй простоті, потужності та величезній екосистемі бібліотек. Його використання дозволяє ефективно автоматизувати процес збору даних, проводити їхній глибокий аналіз, створювати візуалізації та інтегрувати з іншими інструментами та сервісами.

У цьому контексті важливо розглянути ключову термінологію, яка становить основу OSINT-досліджень на Python, і зрозуміти, яку саме роль вони відіграють у дослідницькій практиці.

Почнемо з *веб-скрейпінгу (web scraping)* – процесу автоматичного вилучення даних із веб-ресурсів. Він широко застосовується для збору інформації з публічних профілів у соціальних мережах, витягування новин, статей, контактів або технічних даних з сайтів. Python дозволяє робити це швидко і масштабовано, зокрема за допомогою бібліотек *requests*, *BeautifulSoup* або фреймворку *Scrapy*.

Далі йде *API (Application Programming Interface)* – набір правил і протоколів для отримання доступу до функцій чи даних інших сервісів. У контексті OSINT Python використовується для взаємодії з API таких платформ, як Twitter, Facebook, YouTube, TikTok або Google Maps. Це дозволяє отримувати структуровану інформацію напряму – швидше і точніше, ніж з HTML-сторінок.

Зібрані дані часто потребують розбору. Саме тут важливу роль відіграє *парсинг (parsing)* – обробка й аналіз текстових чи структурованих даних *наприклад* (HTML, JSON, XML) для вилучення потрібних елементів. У практиці OSINT це може бути витягування адрес електронної пошти, імен користувачів, номерів телефонів, фото, відео та іншої значущої інформації.

Інший напрям – *геолокація (geolocation)*. Python дозволяє аналізувати IP-адреси, координати чи EXIF-метадані фотографій, щоб визначити географічне розташування об'єкта. Це важливо в дослідженнях, які пов'язані з відстеженням місця перебування людей, техніки чи подій.

На основі отриманих даних може будуватися і більш глибокий аналіз, зокрема в межах *соціальної інженерії (social engineering)* – методу, що використовує відкриті дані для вивчення, моделювання або маніпуляції поведінкою людей. Python може допомогти систематизувати та візуалізувати такі дані, *наприклад*, у формі зв'язків між особами або організаціями.

Крім того, важливе місце в OSINT-процесах займає автоматизація (automation). Python дозволяє створювати скрипти, які періодично перевіряють зміни на сайтах, надсилають запити до API, зберігають результати та навіть надсилають сповіщення. Це дає змогу уникнути рутинної роботи й оперативно реагувати на нову інформацію.

У більш складних сценаріях аналітики застосовують *OSINT-фреймворки* – готові набори інструментів, написаних на Python. До них належать, *наприклад*, *SpiderFoot* (для автоматизованого збору понад 100 типів даних), *theHarvester* (для пошуку доменів, email-адрес), *Social Analyzer* (модульна платформа OSINT) тощо. Вони поєднують у собі можливості збору, фільтрації, аналізу та візуалізації інформації, часто з інтеграцією з базами даних або зовнішніми сервісами.

Таким чином, Python у сфері OSINT – це не просто мова програмування, а ціла екосистема, що дозволяє реалізовувати завдання будь-якої складності: від

простої автоматизації збору відкритих даних до складного аналізу зв'язків, тональності, геолокації та поведінкових патернів. Його гнучкість і підтримка великою спільнотою перетворюють Python на один із головних інструментів сучасного дослідника у сфері інформаційної безпеки та розвідки з відкритих джерел.

Серед великої кількості інструментів, доступних дослідникам у сфері OSINT, особливе місце займає *Social Analyzer* – потужний Python-інструмент, орієнтований на пошук і аналіз профілів у соціальних мережах. Його основне призначення – ідентифікація цифрового сліду особи за іменем користувача або ключовими словами у великій кількості платформ.

Social Analyzer – це API, CLI та веб-додаток, який дозволяє здійснювати пошук і аналіз профілю людини в понад 1000 соціальних мережах, він також включає різні модулі аналізу та виявлення, які користувач може вибирати під час розслідування (*рис.1*).

Особливістю Social Analyzer є *використання спеціальних методів виявлення*, що дозволяють здійснювати цілеспрямований пошук у таких джерелах:

- **Facebook** – за номером телефону, іменем або назвою профілю
- **Gmail** – за адресою електронної пошти (наприклад, example@gmail.com)
- **Google** – за будь-якою email-адресою (наприклад, example@example.com)

Модулі пошуку оцінюють знайдені збіги за допомогою різних методів і присвоюють їм рейтинг від 0 до 100. Залежно від цього результат позначається як *«Ні»*, *«Можливо»* або *«Так»*. Це дозволяє зменшити кількість помилкових відповідей і підвищити точність, тому знайдений результат з високою ймовірністю може бути релевантним.

Посилання на ресурс для завантаження інструменту *Social Analyzer* – *https://github.com/qeeqbox/social-analyzer*

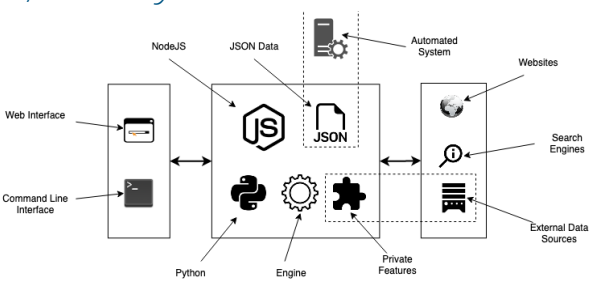


Рисунок 1. Структура проєкту Social Analyzer

Доступний функціонал:

- *аналізує імена та слова*, наприклад знаходить різні варіанти написання або перестановки букв у імені;
- *здійснює пошук профілей людей в інтернеті*, використовуючи кілька способів, зокрема автоматичні браузери;
- *перевіряє кілька профілів одночасно*, щоб знайти, чи пов'язані вони між собою;
- *розпізнає текст на зображеннях*, навіть якщо текст складний або прихований;
- *показує інформацію у зручній візуальній формі*, наприклад у вигляді діаграм або схем;
- *отримує приховані дані із профілів та сайтів*, наприклад метадані, які не видно звичайному користувачу;
- *будує зв'язки між даними*, щоб зрозуміти, як пов'язані різні профілі або сайти;
- *здійснює пошук сайтів за країною*, рейтингом чи тематикою, наприклад музика, дорослий контент тощо;
- *аналізує популярність профілів* і виводить статистику;

РОЗДІЛ 18

ФІНАНСОВА АНАЛІТИКА КОМПАНІЙ З МЕДІЙНИМ СЛІДОМ В YouTube

Сергій БОРТНИК
Анатолій Тімошин

ІНТЕГРАЦІЯ ФІНАНСОВИХ І РЕПУТАЦІЙНИХ ІНДИКАТОРІВ

Побудова фінансово-репутаційного дашборда компанії дозволяє аналізувати компанію одночасно з фінансової та репутаційної перспектив. Фінансові дані компаній – як основа, YouTube – як додаткове джерело OSINT (медійний слід). Такий дашборд дозволить поєднати кількісні фінансові показники з якісними ознаками публічного іміджу компанії, що в сукупності створює ширший контекст для прийняття управлінських рішень, інвестиційного аналізу або оцінки ризиків.

Ключова ідея поєднання фінансів і медіа-аналітики полягає в тому, що сильний негативний інформаційний фон дуже часто передує або супроводжує фінансові втрати, втрату довіри, відтік інвесторів. Якщо компанію регулярно згадують у скандальному чи негативному ключі, і водночас у неї падають прибутки (росте борг), зменшуються активи – це прямий сигнал для інвесторів. Якщо ж згадуваність росте, але фінанси стабільні – це може бути інформаційна атака або PR-війна. Дашборд можна розглядати як оцінку стабільності партнера або конкурента. Це може бути корисним для служби безпеки або аналітичного відділу, коли потрібно перевірити контрагента (*наприклад*, при держзакупівлі) – у партнера хороші фінпоказники, але в інфопросторі – десятки відео про підозри у схемах. Або навпаки: позитивний піар, але фінансова яма – ризик невиконання зобов'язань. Це виявлення штучного піару або прихованого інформаційного впливу. Якщо є раптові піки згадок у YouTube – і це не пов'язано з реальними фінансовими подіями, це може бути замовний піар, відволікання уваги від внутрішніх проблем.

При наявності даних по кількості згадок в YouTube та фінансових результатах (доходи, EBITDA, акції) можна дослідити чи впливають інфохвилі на прибутки, чи падає довіра до компанії після скандалів, як змінюється структура згадок після зміни керівництва.

Зауважимо, що ідеальна логіка OSINT-аналітики – це виявити *індикатори на основі відкритих джерел*, які передують подіям, і потім підтвердити їх фактичним результатом (*наприклад*, показниками фінансового стану). Такий підхід навіть має назву – *«Retrospective validation of OSINT indicators»* (*Ретроспективна валідація індикаторів OSINT*).

У процесі оцінки компанії з урахуванням фінансової інформації та медійного сліду доцільно розрізняти три ключові компоненти: *ризик-оцінку, скоринг* та *дашборд*.

Ризик-оцінка (risk assessment) – це комплексний процес аналізу ймовірних загроз, що можуть впливати на стійкість компанії. Вона включає фінансові, операційні, регуляторні та репутаційні чинники. Використовуються як кількісні (показники, ймовірності), так і якісні (думки експертів) методи. Це найширше поняття серед трьох.

Скоринг (scoring) – це результат формалізованої (кількісної) оцінки ризику за допомогою математичної або машинної моделі. Скоринг відображає підсумковий бал або рейтинг, що дозволяє класифікувати об'єкти за рівнем ризику. Скоринговий бал, як зведена оцінка, може коливатись від 0 до 1. *Наприклад*, 0.93 – дуже надійний, 0.42 – підвищений ризик. Взагалі, градація

скор-балів компанії наступна – низький ризик (0.8–1.0), середній ризик (0.4–0.79), високий ризик (0.0–0.39).

Дашборд (dashboard) – це візуальний інструмент, який об'єднує результати аналізу та скорингу в інтерактивному форматі. Він надає змогу швидко оцінити поточний стан компанії, спираючись на дані з різних джерел – фінансових, медійних, репутаційних. Передбачає графіки, таблиці, індикатори ризику, скоринг-бали, сценарії порівняння.

Слід зауважити, що *індикатори на дашборді* – це візуальні елементи, які показують поточні значення окремих метрик. *Наприклад*: прибуток, виручка, кількість згадок у ЗМІ, індекс токсичності новин, тощо. Індикатори не є результатом моделі, а просто показують окремі дані або KPI (*Key Performance Indicator – ключовий показник ефективності*). *Мета індикаторів* – моніторинг, відстеження трендів, а не рішення. Але, вони можуть бути вхідними даними для скорингу. Отже, *скоринг – це аналітичний результат, а індикатор – окремий факт або метрика*. Вони взаємодіють, але мають різну функцію.

Отже, надалі будемо спиратись на наступну архітектуру майбутнього дашборду (*рис. 1*).

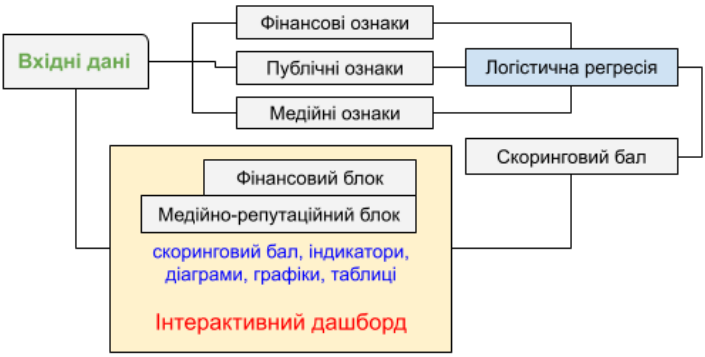


Рисунок 1. Архітектура дашборду

МОДЕЛІ СКОРИНГУ

Зупинимось окремо на моделях скорингу. Найпоширеніша та найбільш прозора модель – це класичний статистичний скоринг (логістична регресія). Формула логістичної регресії наступна:

$$P = \frac{1}{1 + e^{-(\beta_0 + \beta_1 x_1 + \ldots + \beta_n x_n)}}$$

де P – ймовірність невиконання зобов'язань, x_i – вхідні характеристики (вік, дохід, кредитна історія), β_i – вагові коефіцієнти моделі.

Рейтингові правила (rule-based scoring). Простий набір правил «якщо – тоді». *Наприклад*, Якщо вік компанії менше 2о років, то це: -50 балів, якщо немає прострочок за останні 12 місяців, то: +100 балів, якщо зарплата перевищує 30 000 грн., то: +80 балів, і т.п. Така модель добре підходить для первинного фільтру і не адаптується до нових даних про компанію.

Дерева рішень та ансамблі (Decision Tree, Random Forest, XGBoost, LightGBM). Вхідні дані: кредитна історія, доходи, соцмережі, поведінка онлайн. Вихід: ймовірність дефолту, клас ризику. Ця модель навчається на історичних даних і обробляє не лінійні взаємозв'язки.

Моделі машинного навчання (ML). Для фінансового скорингу використовуються алгоритми *SVM (Support Vector Machine)*, *KNN (K-Nearest Neighbors)*, *Naive Bayes (байєсівська модель із припущенням незалежності ознак)*. Прикладом ML є нейронні мережі, які здатні виявляти складні нелінійні залежності. Особливо

«OSINT – це не лише інструмент розслідування. Це архітектура цифрової справедливості, де кожен фрагмент даних – цеглина у доказовому фундаменті правди»
- Авторська формула

У сучасному світі, де війна точиться не лише на полі бою, а й у цифровому просторі, відкриті джерела інформації стали зброєю правди. OSINT – це не лише технологія, це методологія, що дозволяє бачити те, що приховано, і документувати те, що заперечується. Його застосування особливо важливе у розслідуваннях воєнних злочинів, цифрової доказовості, біометричної ідентифікації та аналізу інформаційних слідів.

Цифрові фрагменти – голос, фото, номер, акаунт – можуть стати ключем до встановлення істини, коли традиційні методи безсилі. Як слушно зазначав Карл Поппер, «*правосуддя починається з факту. А факт – це те, що доведено*». Саме тому ця частина посібника зосереджена на практичних рішеннях, які перетворюють дані на докази.

Зібрані тут українські та міжнародні інструменти – від аналізу мобільних пристроїв до візуалізації зв'язків – формують основу цифрової криміналістики. Це не просто перелік ресурсів, а архітектура цифрової справедливості, де кожен елемент – цеглина у фундаменті відповідальності. Частина стане дороговказом для слідчих, аналітиків, прокурорів і кіберфахівців, які працюють на перетині технологій, права та безпеки.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ OSINT ЗА ОКРЕМИМИ НАПРЯМАМИ РОЗСЛІДУВАННЯ

ЧАСТИНА IV

РОЗДІЛ 19

ЦІЛЬОВІ OSINT РЕСУРСИ ДОКУМЕНТУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

Дмитро ХУДЕНКО

До даного огляду прикладних ресурсів, які сприяють притягненню до відповідальності за воєнні злочини в Україні, увійшли, як публічні, так і приватні ресурси, більшість з яких є українські, а також – європейські та російські. Перелік охоплює період їх створення 2014 – 2022 роки та орієнтується на використання цільових методів та джерел інформації, більшість з яких є відкритими та не втратили свою актуальність і до сьогодні.

№ п/п	Назва	QR-code	Опис та посилання
1	CIVILIAN HARM IN UKRAINE		Зібрання та відображення на спеціальній карті груп подій в Україні, пов'язаних із шкодою цивільному населенню, а також втратами серед нього унаслідок збройного конфлікту після 24 лютого 2022 року. *https://ukraine.bellingcat.com/*
2	DAILY TACTICAL UPDATE		Каталог оновлюваних ситуаційних карт із розташуванням сторін у російсько-українській війні від одного із дослідників людських конфліктів *https://x.com/JominiW*
3	DEEPSTATEUA		Інтерактивна онлайн мапа бойових дій в Україні. *https://deepstatemap.live/*
4	EVOCATION		Збірка інформації щодо російських пропагандистів та поплічників окупаційного режиму рф. *https://evocation.info/uk/*
5	EYES ON RUSSIA		Некомерційній соціальний проект для збору, аналізу та перевірки відео, фотографій, супутникових знімків або інших медіа, пов'язаних із вторгненням Росії в Україну *https://eyesonrussia.org/*
6	INTERNATIONAL PARTNERSHIP FOR HUMAN RIGHTS		Повідомлення щодо порушень прав людини у світі, зокрема, під час воєнних дій на території України. *https://iphronline.org/*
7	HACKYOURMOM		Ряд розділів містить не лише інформацію про цифрові сили та засоби, пов'язані із протидією російській агресії, але й результати досліджень та заходів, спрямованих на нанесення нападнику максимальної шкоди за всіма можливими напрями, починаючи з інформаційно психологічного та хакерського напряму, закінчуючи розвідувально бойовим. *https://hackyourmom.com/*

38. Які можливості надає користувачам цей ресурс?
39. Що таке *«Миротворець»* і коли він був створений?
40. Які джерела даних використовує *«Миротворець»*?
41. Які типи класифікацій застосовуються до осіб у базі *«Миротворця»*?
42. Назвіть приклади категорій, за якими класифікуються особи в *«Миротворці»*.
43. Які додаткові сервіси інтегровані у веб-портал *«Миротворець»*?
44. Що таке NEUROIDENTIGRAF і як він працює?
45. Які технічні вимоги висуваються до фотографій для розпізнавання облич?
46. Які обмеження має інтерфейс *«Миротворця»*?
47. Які країни є основними джерелами трафіку на сайт *«Миротворець»*?
48. Які переваги та недоліки має ресурс з точки зору OSINT-аналітика?
49. Які етичні та правові виклики пов'язані з використанням таких ресурсів?
50. Як ресурси *«Книга катів»* і *«Миротворець»* сприяють документуванню воєнних злочинів?
51. Які типи доказів можуть бути зібрані через ці платформи?
52. Чому ці ресурси важливі для інформаційної безпеки та історичної пам'яті України?

РОЗДІЛ 20

ПРОЦЕСУАЛЬНІ МЕХАНІЗМИ ЗБИРАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ ЩОДО ВОЄННИХ ЗЛОЧИНІВ

Христина ПОДИРЯКО
Людмила ГАВРИЛЮК
Дмитро ШЕВЧУК

Одночасно із повномасштабним вторгненням рф на територію нашої держави, нагальною необхідністю для слідчих стало правильно документувати такі протиправні дії, й забезпечувати в такий спосіб виконання завдань кримінального провадження. На сьогодні, у значній кількості випадків доводиться проводити досудове розслідування воєнних злочинів у дистанційному режимі, що з однієї сторони, дозволяє збирати докази, убезпечуючи від їх знищення чи втрати, а з іншої сторони – вимагає нових ґрунтовних методик і алгоритмів, які мають бути дороговказом для слідчих.

На якість розслідування воєнних злочинів впливає ряд негативних чинників, які ніяким чином не залежать від діяльності слідчих, а саме:

1) *обмежений, а в деяких випадках відсутній доступ до тимчасово окупованих територій та територій у «сірій» зоні, що унеможливлює завчасне проведення слідчих (розшукових) дій;*
2) *відсутній доступу до місця злочину на окупованій території, у зв'язку з чим відсутня можливість вчасно зібрати речові докази, які з часом можуть бути пошкоджені, або повністю знищені;*
3) *недостатньо інформації про військовослужбовців рф у наявних базах даних правоохоронних органів;*

4) *відсутня можливість проведення слідчих (розшукових) дій із підозрюваним/обвинуваченим, який перебуває на тимчасово окупованій території, території рф, Республіки Білорусь та в країнах іншої юрисдикції;*
5) *втрата доказів у зв'язку із відсутністю налагодженої взаємодії з працівниками інших правоохоронних органів, військовими, які першими потрапляють на місце злочину;*
6) *недотримання процесуального порядку отримання доказів, що призводить до отримання недопустимих доказів, використання яких, може привести до утворення великої кількості недопустимих доказів за принципом «плодів отруйного дерева»;*
7) *складнощі при ідентифікації безпосередніх виконавців вчинення злочинів;*
8) *можливість повторних ударів в момент проведення слідчих (розшукових) дій;*
9) *заміновані місця вчинення воєнних злочинів;*
10) *існують ризики знищення матеріалів кримінальних проваджень та речових доказів внаслідок ударів по об'єктам, де вони зберігаються;*
11) *велика латентність злочинів, тощо.*

Названі фактори істотно впливають на ефективність розслідування, створюють дефіцит можливостей для отримання традиційних доказів. Практичний досвід розслідування воєнних злочинів засвідчує ефективність комплексного підходу до збирання доказів і методів їх аналізую.

На початковому етапі розслідування воєнних злочинів, окрім допиту потерпілих, свідків, проведення інших першочергових СРД та НСРД, одним з основних завдань слідчих *є встановлення підрозділів збройних сил рф, які перебували на місці вчинення кримінального правопорушення, у визначений період*. Це стає можливим унаслідок проведення комплексу заходів, зокрема дослідження деокупованих територій з метою пошуку та вилучення документів, мобільних пристроїв, залишених окупантами, робота з полоненими, аналіз мобільного трафіку російських військовослужбовців, отримання інформації від розвідувальних органів.

На цьому етапі розслідування особливу увагу слід приділити дослідженню деокупованої території. З метою виявлення та фіксації доказів вчинення злочину слідчий має провести детальний огляд місця події. Одним із завдань слідчого під час проведення СРД-огляду є виявлення та вилучення наявних носіїв інформації в електронній (цифровій) формі, на яких можуть бути зафіксовані злочини, які вчиняли військовослужбовці рф на території України, інформація, яка може стати інструментом для ідентифікації та зіставлення військової техніки, встановлення типу військової техніки та озброєння, ідентифікації зафіксованих військовослужбовців рф, встановлення їх анкетних даних, місця проживання, паспортних даних, встановлення їх сторінки у соціальних мережах, актуальних фото, які можна буде використати під час пред'явлення особи для впізнання за фотознімком, можливі номери мобільних телефонів російських військовослужбовців/їх близьких родичів, друзів та іншу інформацію, яка може бути важлива для проведення повного, швидкого та неупередженого досудового розслідування, встановлення всіх обставин кримінальних правопорушень і винних осіб.

Така інформація може бути зафіксована камерами відеоспостереження, які встановлені на будівлях, вулицях населених пунктів деокупованих територій, у засобах фото- та відеозапису на БПЛА, у виявлених на місці події ноутбуках, мобільних пристроях, якими могли користуватися військовослужбовці рф тощо. У разі виявлення таких носіїв інформації в електронній (цифровій) формі слідчі мають вжити заходи щодо належного їх вилучення і збереження інформації, яку там розміщено. Надалі така інформація підлягає детальному аналізу з метою встановлення обставин, які мають значення у кримінальному провадженні.

підозрюваних. Таким чином, цифрові докази стають ключовим елементом у доведенні причетності до воєнних злочинів, а їх належне документування – запорукою ефективного кримінального провадження.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Які основні виклики виникають під час розслідування воєнних злочинів в умовах збройної агресії?
2. Чому досудове розслідування часто проводиться у дистанційному режимі?
3. Які ризики пов'язані з недотриманням процесуального порядку збирання доказів?
4. Що означає принцип *«плодів отруйного дерева»* у кримінальному процесі?
5. Які джерела електронних доказів можуть бути виявлені на деокупованих територіях?
6. Які типи інформації можуть містити мобільні пристрої військовослужбовців рф?
7. Які заходи слід вжити для збереження даних на мобільному пристрої?
8. Чому не можна вимикати увімкнений мобільний пристрій під час огляду?
9. Що таке IMEI-код і яку роль він відіграє у розслідуванні?
10. Яку інформацію може містити SIM-карта?
11. Як за допомогою мобільного телефону можна встановити місцезнаходження підозрюваного?
12. Що таке негласна слідча дія щодо встановлення місцезнаходження радіообладнання?
13. Які процесуальні дії дозволяють отримати дані від мобільних операторів?
14. Які підрозділи Національної поліції залучаються до аналізу абонентських номерів?
15. Як можна використовувати соціальні мережі для ідентифікації військовослужбовців рф?
16. Які методи пошуку за зображенням описано у розділі?
17. Які метадані можна отримати з цифрового зображення?
18. Які інструменти розпізнавання облич згадано у розділі?
19. Які ознаки можуть свідчити про недостовірність відео?
20. Чому цифрові докази є критично важливими у справах про воєнні злочини?

РОЗДІЛ 21

ІДЕНТИФІКАЦІЯ ОСОБИ ЗА ГОЛОСОМ У КРИМІНАЛЬНИХ РОЗСЛІДУВАННЯХ

Денис ПЕФТІЄВ

Голос може бути потужним ідентифікатором. У правоохоронній діяльності *судова ідентифікація голосу* (також відома як розпізнавання диктора або голосова біометрія) – це сукупність методів, які визначають, чи певний зразок голосу (з телефонного дзвінка, запису тощо) відповідає відомій особі або розкриває характеристики диктора. Оскільки злочинці все частіше спілкуються через

кордони за допомогою голосу (телефонні дзвінки, інтернет-дзвінки, записи з вимогами викупу тощо), такі агентства, як ІНТЕРПОЛ, ЄВРОПОЛ, ФБР та інші, звернулися до передових технологій, включаючи *розпізнавання голосу на основі ШІ та навіть великі мовні моделі (LLM)*, для допомоги в розслідуваннях.

ІСТОРИЧНИЙ ОГЛЯД ІДЕНТИФІКАЦІЇ ГОЛОСУ В КРИМІНАЛІСТИЦІ

Ранні спроби ідентифікувати злочинців за їхнім голосом сягають багатьох десятиліть. Один відомий приклад стався в 1932 році під час викрадення дитини Ліндберга: Чарльз Ліндберг почув голос того, хто вимагав викуп, і *через три роки засвідчив*, що голос належав Бруно Гауптманну, обвинуваченому у викраденні. Цей випадок стимулював науковий інтерес до розпізнавання голосу. У 1936 році дослідниця Френсіс МакГі провела одне з перших досліджень з ідентифікації голосу, виявивши, що здатність людей розпізнавати незнайомий голос з часом значно знижується, що підкреслює *обмеженість людської пам'яті на голоси*.

Сучасна судова ідентифікація голосу по-справжньому почалася в середині 20-го століття з появою *звукового спектрографа* (пристрою, який візуально представляє звукові частоти в часі). Під час Другої світової війни аудіоспеціалісти армії США розробили ідею «голосових відбитків» для ідентифікації ворожих радіооператорів, сподіваючись відстежувати переміщення, розпізнаючи один і той самий голос у різних місцях. Після війни *фізик з Bell Labs Лоуренс Г. Керста* став піонером застосування спектрографічної ідентифікації голосу для правоохоронних органів. У 1962 році Керста ввів термін *«voiceprint» (голосовий відбиток)* і опублікував метод візуального порівняння патернів мовленнєвих спектрограм для ідентифікації дикторів. Поліція та дослідники побачили перспективу у зіставленні унікальних патернів голосового тракту людини – по суті, акустичного відбитка пальця.

Перші судові справи, що використовували голосові відбитки, з'явилися в 1960-х роках. *Наприклад*, поліція Нью-Йорка залучила Керсту для аналізу телефонних погроз про закладення бомб. В одній примітній справі близько 1966 року підозрюваного в підпалі було ідентифіковано шляхом порівняння запису його інтерв'ю у в'язниці з невідомим голосом у новинах CBS – Керста засвідчив, що голоси збігаються, і підозрюваного було засуджено. Однак цей вирок було скасовано в апеляції, оскільки суд визнав аналіз голосових відбитків ще не науково обґрунтованим. Аналогічно, у 1976 році Верховний суд Каліфорнії (у справі People v. Kelly) відхилив докази на основі спектрографії голосу, «доки не буде продемонстровано вагомого наукового схвалення на їх підтримку». *Ці ранні юридичні проблеми підкреслили скептицизм щодо надійності – ідентифікацію голосу порівнювали з ранніми днями дактилоскопії, яка потребувала більшої валідації*.

Незважаючи на невдачі, дослідження в галузі судової ідентифікації голосу тривали. До 1980-х років лабораторії правоохоронних органів (*наприклад*, Департамент шерифа округу Лос-Анджелес) почали високотехнологічні проєкти для наукової валідації голосових відбитків за допомогою комп'ютерів. Переходячи від суто візуального зіставлення патернів, вони розробили комп'ютеризовані системи для аналізу голосових патернів з більшою об'єктивністю та статистичною строгістю. З часом методологія розвинулася від порівняння кількох слів на паперових спектрограмах до комплексного аналізу всіх аспектів мовлення, поєднуючи аудіальне (слухове) та спектрографічне дослідження. До 1990-х і 2000-х років багато судів стали більш прихильними до експертних свідчень з порівняння голосів, за умови, що використовувані методи були валідовані та пояснені. Коротко кажучи, *історична траєкторія рухалася від примітивних аналогових методів «голосових відбитків» до більш стандартизованих, науково обґрунтованих технік, що підготувало ґрунт для сучасних цифрових та ШІ-керованих підходів*.

Розділ 22

КЛАСИФІКАЦІЯ OSINT-РЕСУРСІВ ЗА ЦІЛЬОВИМИ ЗАВДАННЯМИ РОЗСЛІДУВАННЯ

Юрій КРУТІК

У сучасному цифровому середовищі ефективне розслідування злочинів, особливо в умовах війни, неможливе без використання спеціалізованих OSINT-інструментів. Від збору даних у соціальних мережах до аналізу великих масивів інформації – кожен етап потребує точних, адаптованих рішень. Цей розділ систематизує понад 100 ресурсів, платформ і сервісів, які використовуються для відкритої розвідки, класифікуючи їх за функціональними ознаками: аналітичні системи, пошукові платформи, інструменти розпізнавання, агрегатори персональних даних, реєстри, розширені пошуковики, email-трекери, IMEI-аналізатори тощо.

Такий підхід дозволяє слідчим, OSINT-аналітикам, журналістам-розслідувачам та кіберфахівцям обирати інструменти відповідно до конкретного завдання: ідентифікація особи, перевірка контрагента, аналіз цифрового сліду, візуалізація зв'язків, виявлення витоків даних. Розділ також містить приклади українських розробок, що демонструють високий рівень технологічної адаптації до умов війни та потреб національної безпеки.

Посилання	Опис	Назва
	OSINT-системи	
https://harvester-ai.com/	Платформа на базі ШІ для автоматичної обробки та аналізу великих обсягів цифрової інформації, що розроблена українською командою MATHESIS спеціально для органів державної безпеки. Продукт допомагає швидко фільтрувати та оперативно знаходити потрібну інформацію в океані неструктурованих даних.	Mathesis HARVESTER
https://youcontrol.com.ua/	українська аналітична онлайн-система для бізнесової аналітики, конкурентної розвідки та перевірки контрагентів.	YouControl
https://strabis.com.ua/web2w/login.php	українська аналітична платформа, розроблена для пошуку, обробки та аналізу інформації з різних джерел, як структурованих (бази даних), так і неструктурованих (наприклад, Інтернет).	Страбіс
https://youscan.io/product/?utm_source=google&utm_medium=cpc&utm_campaign&utm_term&hsa_acc=5914147660&hsa_cam=21040427974&hsa_grp=156959815817&hsa_ad=691334376912&hsa_src=g&hsa_tgt=dsa-2275706968742&hsa_kw&hsa_mt&hsa_net=adwords&hsa_ver=3&gad_source=1&gbraid=0aaaaacrilpomai6pm9qpoh56b6jwnh_ju&gclid=cj0kcqjwtplabhc7arisalbocvpoztuxkuecwwzdksb2mtanlw-_omh0yp2-soa0jeun12qxsdb_5bgaaqsdealw_wcb	українська аналітична платформа для моніторингу соціальних медіа, яка використовує штучний інтелект для аналізу текстового та візуального контенту. Вона допомагає брендам, агентствам і дослідникам отримувати глибокі інсайти про споживачів, управляти репутацією та приймати обґрунтовані маркетингові рішення.	YouScan
https://www.rakia.ai/	це рішення для управління даними та аналітики, яке використовується для збору, обробки і аналізу даних з різних джерел.	Rakia
https://www.palantir.com/	Програмне забезпечення, яке використовується переважно державними установами та службами безпеки для аналізу даних і виявлення загроз. Воно дозволяє користувачам інтегрувати різноманітні джерела даних та виявляти закономірності та аномалії.	Palantir
https://shadowdragon.io/	надає інструменти для роботи з уже відкритими джерелами або витоками.	Shadow Dragon
https://siren.io/	платформа, яка об'єднує пошук, зв'язки та аналітику даних у реальному часі. Її часто називають «розвідкою на базі Elasticsearch", бо вона побудована поверх Elasticsearch	Siren.io
https://datawalk.com/	це платформа для аналізу зв'язків і великих обсягів даних, яка використовується для OSINT, кримінальних розслідувань, аналітики загроз, фінансової безпеки та розвідки.	DataWalk
https://www.maltego.com/	потужний інструмент для графового аналізу зв'язків між об'єктами.	Maltego
https://i2group.com/	рішення для візуалізації даних і побудови зв'язків.	i2 ANB / i2 Hub
https://x-scif.info/	Інформаційно-аналітична платформа для OSINT та корпоративної безпеки	X-SCIF
https://www.shi.com/product/42956796/Micro-Focus-IDOL-Intelligent-Data-Discovery	це комплексна платформа, розроблена для обробки, аналізу та вилучення інформації з неструктурованих джерел даних, таких як текст, аудіо, відео та зображення. Використовуючи передові технології штучного інтелекту (AI), машинного навчання (ML) і обробки природної мови (NLP), IDOL дозволяє організаціям перетворювати величезні обсяги неструктурованих даних у ефективний інтелект	Idol MicroFocus
https://www.atlas-technologies.com/	це платформа, орієнтована на урядові та оборонні структури, включаючи правоохоронні органи.	ATLAS

Навчальне видання

OSINT OPEN SOURCE INTELLIGENCE
ІНСТУМЕНТИ ТА МЕТОДИ

НАВЧАЛЬНИЙ ПОСІБНИК

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. 14,38. Зам. № 1811-25/2.
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