МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки

Оксана Олександрівна Онищук

МЕТОДИ ТА ЗАСОБИ ПОШУКУ ІНФОРМАЦІЇ З ВІДКРИТИХ І ОБМЕЖЕНИХ ДЖЕРЕЛ НА ОСНОВІ ТЕХНОЛОГІЇ OSINT

Монографія

Луцьк 2026

УДК 004.056.5

Рекомендовано до друку вченою радою Волинського національного університету імені Лесі Українки (протокол № 3 від 26.02.2026 р.)

Рецензенти:

Лаптєв Олександр Анатолійович, доктор технічних наук, старший науковий співробітник, доцент кафедри кібербезпеки та захисту інформації, факультет інформаційних технологій Київського національного університету імені тараса Шевченка

Багнюк Наталія Володимирівна, доцент кафедри комп'ютерної інженерії та безпеки, кандидат технічних наук, факультету комп’ютерних та інформаційних технологій Луцького національного технічного університету

Пастернак Ярослав Михайлович, доктор фізико-математичних наук, професор кафедри комп'ютерних наук та кібербезпеки Волинського національного університету імені Лесі Українки

Онищук О.О. Методи та засоби пошуку інформації з відкритих і обмежених джерел на основі технології OSINT: монографія. Луцьк ВНУ імені Лесі Українки, 2026. 90 с.

ISBN 979-966-641-…

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ,СИМВОЛІВ ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

OSINT - Open source intelligence (Розвідка відкритих джерел)

CCIRM - Collection coordination intelligence requirements management

AIPI - Associazione Internazionale Professori d'Italiano

SSL - Secure Sockets Layer

TLS - Transport Layer Security

API - application programming interface

IP - Internet Protocol

URL - Uniform Resource Locator

ВСТУП

Розвідка з відкритих джерел (OSINT): сучасний інструмент у світі безпеки та розслідувань. Розвідка з відкритих джерел, або OSINT (Open Source Intelligence), – це не нова, але стрімко еволюціонуюча галузь, яка використовується як державними спецслужбами, так і незалежними дослідниками. За десятиліття своєї історії технології та підходи OSINT значно змінилися, дозволивши зробити її доступною та ефективною не лише для професіоналів, а й для громадськості.

Для України термін OSINT став особливо актуальним із початком повномасштабної російсько-української війни. Завдяки цій технології розвідники та волонтери допомагають виявляти ворожі позиції, документувати воєнні злочини, а також спростовувати фейки та пропаганду. Сьогодні OSINT є вагомою частиною розвідки провідних країн світу, таких як США та Велика Британія, де близько 80% інформації добувається саме з відкритих джерел. У порівнянні з 2002 роком, коли в документах НАТО ця частка становила 10-20%, очевидний прогрес.

Основна перевага OSINT – це доступність. Для використання цієї методики не обов'язково працювати в державних розвідувальних структурах чи міжнародних організаціях на кшталт Bellingcat. Завдяки відкритим джерелам, таким як пошукові системи, соціальні мережі чи публічні бази даних, OSINT дає змогу швидко і законно збирати, аналізувати та використовувати інформацію для прийняття рішень або розслідувань.

OSINT – це технологія збору військової, політичної, економічної та іншої інформації з відкритих джерел. Ці джерела включають: пошукові системи (Google, Bing), соціальні мережі (Facebook, Instagram, Twitter), публічні реєстри, новинні портали та веб-сайти компаній. Цей підхід особливо ефективний, коли важливо зберегти конфіденційність розслідування. Наприклад, отримання інформації про компанію або

людину через її активність у соціальних мережах зазвичай є менш помітним, ніж традиційні методи спостереження.

Ризики та етичні аспекти. Сьогодні кожен залишає цифровий слід, працюючи в Інтернеті, навіть не усвідомлюючи цього. Геолокація, робочі години, вподобання в соціальних мережах – все це може стати частиною вашого цифрового профілю. Тому важливо дотримуватись етичних норм і законодавства під час використання OSINT.

Нові можливості OSINT. Сучасні технології спрощують процес збору та аналізу інформації, можливість працювати з величезними обсягами даних у короткі терміни, використання відкритих джерел виключає потребу у складних або секретних методах, OSINT застосовується в кібербезпеці, правоохоронній діяльності, військових операціях та навіть бізнес-розвідці.

Розвідка з відкритих джерел уже стала невід'ємною складовою сучасного світу. Вона дозволяє не лише ефективно реагувати на виклики, але й попереджати загрози, забезпечуючи швидке, законне та результативне використання інформації.

Актуальність роботи полягає у можливості сучасних методів пошуку та аналізу інформації, особливо в умовах стрімкого розвитку цифрових технологій та зростаючої потреби у швидкому доступі до даних. Використання технологій OSINT (Open Source Intelligence) є надзвичайно важливим як для забезпечення інформаційної безпеки, так і для широкого спектра застосувань у бізнесі, політиці, журналістиці та правоохоронній діяльності. Можливість отримання інформації з відкритих і закритих джерел надає нові підходи до досліджень і аналізу, що сприяє прийняттю обґрунтованих рішень і покращенню стратегічного планування.

Мета роботи полягає у дослідженні та впровадженні сучасних методів пошуку й аналізу інформації з відкритих і закритих джерел, а також у застосуванні технологій OSINT для їх практичного використання в умовах сучасного інформаційного середовища.

Для досягнення поставленої мети в роботі передбачено виконання таких **завдань**: проаналізувати сучасні методи OSINT та визначити їх основні типи, етапи й особливості застосування; дослідити міжнародний досвід і нормативно-правові засади, що регулюють використання OSINT; оцінити можливості OSINT у контексті виявлення загроз і реалізації превентивних заходів; ознайомитися з наявними фреймворками та програмними інструментами, які підтримують OSINT-дослідження; провести аналіз сучасних підходів до пошуку інформації; визначити ключові інструменти, що застосовуються для роботи з відкритими джерелами; розробити практичні рекомендації щодо вибору методів OSINT залежно від типу та специфіки поставлених завдань.

Об'єкт дослідження: процеси збору, аналізу та використання інформації з відкритих і закритих джерел у сфері кібербезпеки та розвідувальної діяльності.

Предмет дослідження: методи OSINT, інструменти їх реалізації, а також процеси інтеграції та застосування для забезпечення інформаційної безпеки.

Методи дослідження. Використано аналіз наукових джерел і нормативно-правових актів та порівняльний аналіз методів OSINT; проаналізовано практичні кейси та застосування OSINT у різних країнах; моделювання процесів збору та обробки даних; експериментальне тестування та налаштування інформаційних систем.

Практичне значення отриманих результатів полягає в можливості впровадження розроблених підходів та інструментів OSINT у діяльність державних органів, приватних компаній, розвідувальних структур та інших організацій, що здійснюють заходи у сфері кібербезпеки. Реалізація запропонованих методів сприятиме підвищенню ефективності збору та аналізу інформації, покращенню виявлення потенційних загроз і забезпеченню своєчасного реагування на кіберінциденти.

Апробація результатів роботи. Окремі результати роботи доповідались на IX науково-технічній конференції «Інформаційні моделі, системи та технології» (Житомир, ДУ Житомирська політехніка, 30 – 31 березня 2024 р) ,на VII Всеукраїнській науково-технічній конференції у Житомирі (02-03 грудня 2024 року, Державний університет ”Житомирська Політехніка,) на XIII Міжнародній науково-технічній конференції *«Математика. Інформаційні технології. Освіта»* (Луцьк, 31 травня- 2 червня 2024 року), XIX Міжнародної науково-практичної конференції студентів і аспірантів «*Молода наука Волині: пріоритети та перспективи досліджень*», II Міжнародній науково-практичній конференції «*Проблеми комп'ютерних наук, програмного моделювання та безпеки цифрових систем*»(Луцьк, ВНУ імені Лесі Українки, 9 – 11 червня 2025 р.),; XIV Міжнародної науково-практичної конференції «Математика. Інформаційні технології. Освіта» (13-15 червня 2025 р.) Крім того, апробація результатів дослідження здійснювалася під час читання лекцій на курсах для здобувачів спеціальності F5 Кібербезпека та захист інформації, представлена у наступних статтях електронного фахового наукового видання *Кібербезпека: освіта, наука, техніка: “*Криміналістичні дослідження мобільних пристроїв: порівняння апаратно-програмних засобів шифрування мобільного зв'язку”, “Кібербезпека MQTT-з’єднань на прикладі системи автоматизації воріт”, “Відновлення зв'язків між сутностями в схемах баз даних за допомогою PLANTUML TA LLM” та у електронному фаховому науковому виданні: *Інформаційні технології та комп'ютерна інженері*я “Алгоритми пошуку та аналізу інформації з відкритих джерел в умовах кіберзагроз”

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ВИКОРИСТАННЯ МЕТОДІВ ПОШУКУ ІНФОРМАЦІЇ З ВІДКРИТИХ ТА ЗАКРИТИХ ДЖЕРЕЛ. ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО OSINT. ВАЖЛИВІСТЬ OSINT

1.1. Дослідження наявних методів OSINT. Основні типи та етапи OSINT. Види та нюанси та складності OSINT

Дослідження на основі інформації з відкритим вихідним кодом не є новим видом діяльності для провідних країн світу, і в умовах швидкого розвитку інформаційних технологій методи її використання мають стати предметом відповідних досліджень.

Open Source Intelligence (OSINT) — це підхід, методика та набір технологій, що використовуються для збору та аналізу інформації військового, політичного, економічного чи іншого характеру з відкритих джерел у повній відповідності до законодавства. Цей інструмент застосовується для ухвалення рішень у сферах національної оборони, безпеки, а також у розслідуваннях. OSINT охоплює такі етапи, як збір даних, їх реєстрація, аналіз, обробка, зберігання, захист інформації та надання результатів досліджень. Оброблена інформація з відкритих джерел може трансформуватися у важливе знання, яке за певних умов набуває статусу секретної інформації, якщо не належить до категорій, які виключають таку класифікацію [1, 2, 3].

Інформація з відкритих джерел може бути отримана через Інтернет, що включає такі ресурси, як форуми, блоги, соціальні мережі, сайти обміну відео, метадані, геолокаційні дані, IP-адреси, записи Whois, веб-ресурси Даркнету тощо. Також джерелами є дипломатичні документи, релігійні та розвідувальні організації, академічні дослідження, архіви, «сіра література» (звіти, наукові праці, маркетингові дослідження) тощо.

У деяких випадках дані, отримані з відкритих джерел, можуть бути навіть цінішими за секретну інформацію. Це зумовлено такими чинниками:

1. Оперативність. У кризових ситуаціях, особливо в регіонах із обмеженими розвідувальними можливостями, експерти звертаються до телебачення чи Інтернету.

2. Обсяг. Кількість блогерів, журналістів та інших спеціалістів часто перевищує кількість професійних розвідників, що дозволяє створювати ширшу картину подій.

3. Якість. Інформація з відкритих джерел зазвичай менш піддається фальсифікації, ніж звіти, які можуть базуватися на сумнівних даних.

4. Прозорість. Надійність відкритої інформації частіше є зрозумілою, тоді як ступінь достовірності таємної інформації може залишатися невідомою.

5. Простота використання. Відкрита інформація є легкодоступною, тоді як секретні дані часто ускладнені спеціальними обмеженнями.

Інформація з відкритих джерел є ефективною альтернативою дорогим технологіям, як-от супутникова розвідка, і може надати детальні дані, доступні через прості та дешеві засоби, як-от публікації в журналах. Попри існуючі упередження, OSINT забезпечує доступ до різноманітних джерел інформації, які у своїй сукупності значно перевищують цінність даних із медійних ресурсів, завдяки своїй широті та багатогранності.

1.2. Міжнародний досвід та правові підстави використання методів OSINT

Актуальність дослідження інформаційної безпеки в сучасному світі зумовлена стрімким розвитком цифрових технологій, збільшенням обсягів оброблюваних даних та зростанням кіберзагроз. Інформаційна безпека є

одним із ключових аспектів стабільного функціонування організацій, державних установ та приватних користувачів. Зловмисники постійно вдосконалюють свої методи атак, що вимагає розробки нових підходів до захисту інформації та її збереження. У зв’язку з цим наукові дослідження у сфері інформаційної безпеки стають особливо актуальними. Різні автори пропонують різні стратегії захисту даних, розглядають питання кібергігієни, розробляють системи виявлення та запобігання кіберзагрозам. Таким чином, питання інформаційної безпеки потребує глибокого аналізу сучасних викликів та пошуку ефективних рішень для їх подолання.

Швидке зростання цифровізації призводить до збільшення кількості кіберзагроз, таких як хакерські атаки, витоки даних, фішинг та шкідливе програмне забезпечення. Робота R. Khan *et al*. [15]

надає детальне дослідження та аналіз загроз безпеки та конфіденційності, з якими стикаються мережі 5G, а також розглядає існуючі та перспективні підходи до їх вирішення. Вона підкреслює важливість безпеки як ключового аспекту для широкого впровадження 5G.

Використання відкритих джерел інформації (OSINT) стало ефективним інструментом для збору та аналізу даних з метою виявлення потенційних загроз і їх нейтралізації. Завдяки автоматизованим алгоритмам OSINT можна значно скоротити час на виявлення підозрілих активностей, оцінити рівень ризику і розробити заходи захисту. У роботі M. Bazzell [6, 21, 37] обговорено методи використання відкритих джерел для збору та аналізу інформації з Інтернету, що може оперативно виявляти кіберзагрози, такі як фішинг чи шкідливе програмне забезпечення, а також показано практичні рекомендації для фахівців з кібербезпеки щодо ефективного використання інструментів OSINT для захисту інформаційних систем.

Проблема використання відкритих даних для забезпечення кібербезпеки активно обговорюється в світовій науковій спільноті. А розробники інструментів таких як FOCA [11], Google Search Operators

Cheat Sheet [12], Shodan Report [23, 25], OSINT Framework [22,26,54], Censys [8, 22], Recon-ng [23] надали аналіз поточних глобальних тенденцій в галузі кібербезпеки. Зростаючі кіберзагрози та важливість використання інноваційних технологій для забезпечення стійкості до атак, таких як OSINT і машинне навчання, підкреслили важливість співпраці між державними установами та приватними компаніями для боротьби з кіберзлочинністю. Дослідження останніх років показали значний прогрес у розвитку методів аналізу відкритих джерел. Важливим є застосування таких інструментів, як Recon-ng, Censys та OSINT Framework у роботі Yadav et al. [22, 23, 28, 54], які значно полегшують процес збору даних з інтернет-ресурсів для подальшого аналізу та побудови зв'язків між загрозами.

Інноваційні методи, запропоновані в роботах A. Nagy *et al*. [20], використовували машинне навчання для покращення точності передбачення кібератак на основі даних з відкритих джерел. У статті T. Yang *et al*. [30] розглянуто ефективність алгоритмів виявлення аномалій у цифровому середовищі та важливість автоматизації процесів моніторингу загроз. Це дослідження було зосереджене на використанні байєсівського глибокого навчання для покращення точності виявлення аномалій у кібербезпеці, і завдяки цьому підходу вдалося значно знизити рівень невизначеності в процесах моніторингу та виявлення загроз.

Систематичні огляди T.S. AlSalem et al. (2023) та M.T. Islam et al.[5, 14] були присвячені питанням кібербезпеки в середовищі Інтернету речей (IoT): ризик через вразливості та важливість використання відкритих джерел як засобу виявлення потенційних загроз, типологія загроз, конкретні вразливості та стратегії захисту,. Дані роботи доводять, що обробка відкритих даних у сфері IoT здатна забезпечити побудову прогностичних моделей для раннього попередження атак.

Доповненням до вищезазначених підходів є дослідження D. Kovalchuk [16], яке розкриває потенціал застосування великих мовних моделей (LLM) для автоматизованого аналізу кіберзагроз у корпоративному середовищі, що взято до уваги у поданій роботі. Окрему цінність для поточного дослідження становить робота Ahmed і Patel [29], у якій розглянуто застосування алгоритмів машинного навчання для підвищення ефективності виявлення загроз за допомогою штучного інтелекту. Автори підкреслили переваги інтеграції AI-рішень у системи кібербезпеки, зокрема завдяки здатності таких систем до адаптації, масштабованості й високої точності, що є важливим при побудові архітектури системи виявлення фішингових вакансій. Також, розглянуто роботу J.M Clemen & J. Teleron [9] через розвиток шифрування для захисту комунікацій, тому що шифрування має непрямий вплив на OSINT та для забезпечення цілісності каналів передачі аналітичної інформації [40].

В розглянутій роботі L.K. Vashishtha & K. Chatterjee [27] акцент зроблено на застосуванні природної мовної обробки (NLP) для аналізу текстових даних із соціальних мереж, що може виявляти фішингові кампанії та дезінформацію. Дослідження зосереджувалося на нових методах виявлення загроз за допомогою алгоритмів машинного навчання, зокрема TestCloud IDS і SparkShield, де запропоновано набір даних для тренування алгоритмів для виявлення аномалій та кіберзагроз у хмарних середовищах. У такій роботі M. Alazab *et al*. [4] запропонована удосконалена модель для збору та аналізу даних про загрози, яка може побудувати більш стійкі системи кібербезпеки та використати сучасні інструменти OSINT для прогнозування загроз та зниження ризиків у реальному часі.

Водночас важливим аспектом є проблема достовірності зібраних даних, оскільки велика кількість інформації може бути ненадійною або неперевіреною, що підвищує ризик фальшивих спрацювань системи. Для

подолання цих викликів запропоновано використовувати комбіновані підходи, які поєднують автоматизовані методи з ручною перевіркою даних, що дозволяє підвищити точність результатів. Водночас застосування машинного навчання та штучного інтелекту, як це показано в роботах A.K. Dey *et al*. [10] може знижувати кількість помилкових спрацьовувань і покращувати ефективність виявлення аномалій в реальному часі.

У сучасному світі цифрова інформація (цифрові докази) відіграє ключову роль. У науковій літературі широко застосовується термін “digital evidences” (цифрові докази), який охоплює будь-які дані, збережені чи передані за допомогою комп’ютерної або іншої техніки [6, с. 257]. Іншими поширеними термінами є «електронні докази», «електронні сліди», «цифрові джерела інформації», «електронні документи» тощо. Робота з цифровими доказами вимагає сучасних підходів до їхнього збору, зберігання, аналізу та використання у процесі доказування в кримінальних справах. Застосування цифрової інформації стало одним із інноваційних напрямів розвитку криміналістики та судової експертизи.

Цифрова криміналістика (Digital Forensics) є спеціалізованою галуззю криміналістичної науки та окремим видом судової експертизи. Її основним завданням є дослідження цифрових доказів за допомогою криміналістичних технологій і методик для потреб досудового розслідування та судового процесу [7, с. 129–130]. Ця галузь охоплює процеси збору, отримання, зберігання, аналізу та подання цифрових доказів у межах судових і досудових процедур [46].

Розвиток цифрової криміналістики здійснюється у трьох ключових напрямах: формування самостійної наукової дисципліни в межах криміналістики; застосування спеціальних знань для роботи з цифровими доказами; проведення судових експертиз, включно з комп’ютерно-технічними дослідженнями.

Важливу роль у роботі з цифровими доказами відіграє розробка алгоритмів і правил для їхнього збору, документування та фіксації. Крім того, актуальною є потреба створення криміналістичних методик розслідування міжнародних злочинів, а також рекомендацій щодо запобігання та розслідування конкретних видів правопорушень.

Одним із важливих документів у цій сфері є «Протокол Берклі» (The Berkeley Protocol on Digital Open Source Investigations), який містить рекомендації щодо роботи з цифровими доказами. Розроблений у 2020 році Центром прав людини Університету Берклі та Офісом Верховного комісара ООН з прав людини, цей протокол визначає мінімальні стандарти для збору, зберігання, перевірки та аналізу даних із відкритих джерел. Він слугує практичним посібником для юристів, журналістів, правоохоронних органів і дослідників. Згідно з протоколом, розслідування на основі відкритих даних повністю або частково спираються на загальнодоступну інформацію для вивчення можливих правопорушень, що може підтверджуватися у судах [10].

Серед джерел відкритої інформації: фотографії, відео та інші публікації; контент, створений користувачами соціальних мереж (наприклад, YouTube, Facebook, Instagram); супутникові знімки [14].

Практика використання відкритих джерел інформації (OSINT) є найбільш поширеною в США. Вона застосовується у стратегічних цілях, таких як планування військових операцій, боротьба з тероризмом і забезпечення національної безпеки. Проте основною проблемою OSINT залишається поширення неперевіреної інформації, яка може призводити до хибних рішень. Разом із тим, відкритість цього методу забезпечує можливість міжнародної співпраці без використання секретних методів [6, 37].

Сьогодні OSINT активно використовують правоохоронні органи багатьох країн, такі як США, Велика Британія, Австралія тощо.

Законодавчі ініціативи багатьох держав, зокрема США, підтримують вільний доступ до інформації, створюючи сприятливі умови для розвідки з відкритих джерел. В Україні також декларується свобода інформації (Конституція України, ст. 34). Однак правовий статус OSINT залишається невизначеним, хоча діяльність у цій сфері регулюється низкою законодавчих актів [41].

Розвиток OSINT вимагає системного підходу, включно зі створенням нормативно-правової бази, алгоритмів роботи з інформацією та забезпеченням її достовірності. Це сприятиме ефективному використанню відкритих даних для розслідування, аналітики та забезпечення національної безпеки. [7, 9, 13]

В Україні "кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір" (Конституція України, Розділ 2, ст. 34). В Україні правове регулювання в інформаційній сфері ґрунтується на наступних принципах [2]: свобода законно шукати, отримувати, передавати, виробляти та поширювати інформацію; встановлювати обмеження на доступ до інформації лише законами держави; відкритість інформації про діяльність державних органів та органів місцевого самоврядування та вільний доступ до такої інформації, крім випадків, передбачених законодавством держави; за категорією доступу інформація поділяється на відкриту (загальнодоступну) та з обмеженим доступом.

Разом з тим, узаконеного поняття "OSINT" в Україні сьогодні не існує, хоча діяльність зі збирання, зберігання, обробки та розповсюдження інформації регулюється цілою низкою законодавчих і нормативних актів: Закон України "Про інформацію" від 02.10.92 р. № 2657-XII (зі змінами від 13.01.11 р.), ст. 5–7[2-3]; Закон України "Про друковані засоби масової інформації (пресу) в Україні" від 16.11.92 р. № 2782-XII, ст. 6, 25 [2]; Закон України "Про охоронну діяльність" від 22.03.12 р. № 4616-VI, ст. 9,

13, 19 [13]; Закон України “Про захист персональних даних” № 2297-VI від 01.06.10 р.[14]; Цивільний кодекс України (ст. 505), Кримінальний кодекс України (ст. 231, 232), Кодекс України про адміністративні правопорушення (ст. 163, ст. 163) [1,2,3].

Варто зазначити, що реалізація заходів у частині забезпечення безпеки підприємництва навіть в рамках розвідки з відкритих джерел інформації в окремих випадках сприймається як проведення оперативно-розшукової діяльності, здійснювати яку, згідно із Законом України “Про оперативно-розшукову діяльність”№ 2135-XII від 18.02.1992 р. [1-3] вправі тільки суб’єкти, згадані в окремих статтях зазначених Законів України. У затвердженій Указом Президента України “Стратегії кібербезпеки України” від 15.03.16 р. N96/2016 [3, 4] декларуються основні завдання силовим органам, а також передбачається “створення системи своєчасного виявлення, протидії та нейтралізації кіберзагроз, в тому числі із залученням волонтерських організацій”, все це, безумовно, відноситься до застосування засобів конкурентної розвідки в цій галузі.

При цьому чинним Кримінальним кодексом України передбачена кримінальна відповідальність за незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю, а також за розголошення комерційної таємниці. Однак така інформація виходить за рамки розвідки з відкритим джерелом [31,32].

При досить широкому та неоднозначному трактуванні законодавчих норм будь-які процедури збору, обробки та зберігання інформації про конкурентів, з одного боку, стають практично безкарними, тобто легітимними, а, з іншого боку, є важко доступними для громадян. В українській практиці фактично насправді закритий доступ до великого пласту вільно доступної в інших демократичних державах інформації, наприклад, щодо земельні ділянки, нерухомості (наявної і закладеної), наявність банківських рахунків і т.п. Більшу частину відомостей можна

отримати тільки у результаті консультацій з спеціальними експертами. Нині особливо гостро назріла проблема криміналізації деяких державних служб, які у своїй діяльності використовують розвідку з відкритих джерел.

Практичні тренінги з OSINT та електронних доказів, які проводяться радою Європи в Україні, підкреслюють важливість ланцюга зберігання доказів (chain of custody) та відповідності національному кримінальному процесуальному законодавству й міжнародним стандартам. Зокрема, 12–13 січня 2026 року у співпраці з Тренінговим центром прокурорів України та Національною школою суддів України, за підтримки проєкту Ради Європи CyberUA, відбувся спеціалізований тренінг, присвячений використанню відкритих джерел (OSINT) та електронних доказів у кримінальному процесі, з акцентом на кримінальні провадження щодо воєнних злочинів і грубих порушень прав людини. Це демонструє, що легальність OSINT визначається не лише джерелом інформації, але й процедурними гарантіями збирання та обробки даних, що забезпечують допустимість у суді й захист прав людини. На сьогодні, основними європейськими правовими стандартами в галузі захисту персональних даних є Конвенція Ради Європи "Про захист осіб у зв'язку з автоматичною обробкою персональних даних" від 28 січня 1981 року (ETS №108) та "Пакет захисту даних" Європейського Парламенту та Ради від 27 червня 2016 року [24], які є обов'язковими для всіх держав-членів Європейського Союзу і які є предметом для наслідування в області законодавства, в тому числі, і нашою країною. Країни Євросоюзу мають приводити своє законодавство у відповідність зазначеним правовим стандартам. Право на приватність гарантується Конституцією України. Стаття 32 Конституції України говорить: "Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України". Крім того в Конституції України передбачений захист ще деяких аспектів приватності. Так, стаття 30 Конституції України захищає недоторканність житла

(територіальна приватність), стаття 31 – таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (комунікаційна приватність), стаття 32 передбачає заборону збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди (інформаційна приватність), а стаття 28 передбачає заборону піддавати особу без її вільної згоди медичним, науковим чи іншим дослідженням (захищаючи елементи фізичної приватності). Конвенція РЄ про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року (ратифікована Україною 06.07.2010 р.) визначає положення стосовно передачі через національні кордони за допомогою будь-яких засобів персональних даних, що піддаються автоматизованій обробці або зібраних з метою їхньої автоматизованої обробки.

Паралельно з практичними аспектами, 2025–2026 роки характеризуються посиленою законодавчою увагою до регулювання даних, приватності та використання відкритої інформації в різних юрисдикціях.

1.3. Процес розвідки. Види OSINT за напрямками.

Відкриті джерела (OSINT — Open Source Intelligence) — це джерела інформації, доступні широкому загалу та не потребують спеціальних дозволів або підходів для їх використання [34-37]. Вони є важливими для збору даних, які використовуються в розвідці, аналізі ситуацій, забезпеченні інформаційної безпеки тощо. Приклади **відкритих джерел:**

1. Інтернет-ресурси: веб-сайти, новинні портали, блоги, форуми, соціальні мережі (Facebook, Twitter, LinkedIn, Instagram).
2. Державні та міжнародні організації: офіційні веб-сайти урядів, статистичні агентства, міжнародні організації (ООН, ЄС, НАТО).
3. Публічні бази даних: реєстри компаній, державні реєстри, патентні бази, комерційні реєстри.

4. Наукові публікації та дослідження: статті, дисертації, дослідницькі звіти.

5. Мультимедійні матеріали: відео, фотографії, аудіозаписи, які публікуються на відкритих платформах.

6. Аналітичні матеріали: публікації від аналітичних центрів, блогів експертів, репортажі.

Закриті джерела (також відомі як секретні або закриті інформаційні джерела) — це джерела, доступ до яких обмежений або контрольований і які часто потребують спеціальних дозволів для використання. Закриті джерела зазвичай використовуються органами державної безпеки, розвідками, військовими організаціями для збору та аналізу інформації, яка не є доступною для широкого загалу. Приклади закритих джерел:

1. Державні архіви та документи: документи, що мають гриф секретності (державні таємниці).

2. Військові та розвідувальні агентства: спеціалізовані бази даних та звіти, які використовуються для планування та проведення операцій.

3. Конфіденційні звіти: внутрішні документи компаній, звіти з досліджень, бізнес-плани, що не публікуються у відкритих джерелах.

4. Спеціалізовані бази даних: інформація, доступна лише за ліцензіями або через підписку (наприклад, спеціалізовані фінансові бази, наукові дослідження, які захищені авторським правом).

5. Персональні дані: інформація про фізичних та юридичних осіб, яка обробляється в рамках забезпечення конфіденційності та захисту персональних даних.

Різниця між відкритими та закритими джерелами полягає в доступності, рівні захисту інформації, що міститься в них, і вимогах до збору та використання даних. Відкриті джерела надають легкий доступ до інформації, що може бути корисною для аналізу і планування, тоді як закриті джерела часто вимагають спеціальних дозволів і забезпечують

більш точні та специфічні дані, що можуть мати велике значення у сфері національної безпеки, бізнесу та розвідки.

1.4. Безпечний OSINT. Ризики дослідника. Безпечна платформа для OSINT.

Збір інформації з відкритих джерел (OSINT) може бути надзвичайно корисним, але водночас несе певні ризики для дослідника. Дослідник, що займається OSINT, може стати мішенню для юридичних, кіберзагроз і фізичних атак. Дослідник може зіткнутися з правовими проблемами, якщо інформація, що збирається, суперечить законам або порушує права третіх осіб. Збір інформації з відкритих джерел може спричинити спроби кібератак, які націлені на витік особистих даних дослідника або компрометацію його системи. У разі обробки чутливої інформації або роботи в ризикованих зонах дослідники можуть зазнати фізичних загроз від третіх осіб [42-45].

Дослідникам необхідно використовувати захищені платформи для збору та аналізу даних, щоб мінімізувати ризики. Платформи з відкритим вихідним кодом, які підтримують шифрування і анонімність, наприклад, Spiderfoot або Maltego, можуть забезпечити безпеку під час роботи [19, 26]. Важливо, щоб ці інструменти були налаштовані так, щоб мінімізувати витік даних і забезпечити анонімність користувача. Надійне зберігання паролів є ключовим для забезпечення безпеки OSINT. Для цього необхідно використовувати спеціалізовані менеджери паролів, які зберігають паролі у зашифрованому вигляді та мають функції автозаповнення. Приклади таких програм включають LastPass, 1Password та Bitwarden. Важливо використовувати багатофакторну аутентифікацію (MFA) для додаткового захисту облікових записів [6,13,21, 37].

Використання VPN є важливою практикою для захисту приватності при зборі інформації. VPN створює зашифроване з’єднання між

користувачем і сервером, приховуючи IP-адресу і забезпечуючи захист даних від перехоплення. Це дозволяє досліднику зберігати анонімність під час підключення до Інтернету, запобігаючи тому, щоб його активність була відслідкована третіми особами.

Використання VPN може бути ефективним, але важливо перевіряти, чи не виникають витоки даних (DNS leak), що дозволяють розкрити реальну IP-адресу користувача. Щоб уникнути цього, потрібно:

1. Перевіряти VPN на витоки DNS за допомогою онлайн-інструментів.
2. Використовувати VPN-сервіси, які мають вбудовану функцію захисту від витоків DNS (наприклад, NordVPN, ExpressVPN).

TOR (The Onion Router) — це мережа, яка забезпечує високий рівень анонімності, перенаправляючи інтернет-з’єднання через кілька серверів по всьому світу. Використання TOR допомагає приховати IP-адресу і забезпечити анонімність під час серфінгу, хоча варто пам’ятати, що швидкість з’єднання може бути низькою.

Proxy — ще один інструмент, що дозволяє змінювати IP-адресу користувача. Проксі-сервери можуть бути корисні для обходу географічних обмежень, але для захисту анонімності краще використовувати проксі-сервіси, які не зберігають журнали активності.

Анонімність платежів є важливим аспектом безпеки для дослідників. Використання криптовалют (наприклад, Bitcoin, Monero) або сервісів, які гарантують анонімність транзакцій, може допомогти забезпечити фінансову конфіденційність. Сервіси, як CoinJoin або Wasabi Wallet, додають додатковий рівень анонімності.

Підсумовуючи, для безпечного проведення OSINT-досліджень необхідно використовувати комбіновані методи захисту: VPN, TOR, проксі-сервери, а також анонімні платіжні методи для захисту конфіденційності та безпеки даних.

1.5. Основні можливості OSINT

Основні можливості OSINT (Open Source Intelligence) реалізуються через послідовний і структурований процес збору, аналізу та інтерпретації інформації з відкритих джерел. Для досягнення максимальної ефективності цей процес доцільно представити у вигляді чотирьох взаємопов'язаних етапів, кожен з яких виконує окрему функцію в циклі розвідувальної діяльності [38,39, 45, 48].

1. Визначення цілей та стратегічне планування. Початковий етап передбачає формування чіткої мети дослідження, визначення об'єкта та меж аналізу, а також розробку стратегії збору інформації. На цьому етапі здійснюється постановка конкретних запитань, формулювання ключових слів і пошукових запитів, визначення мовного контексту та часових рамок дослідження. Крім того, відбувається ідентифікація релевантних джерел інформації (веб-ресурсів, соціальних мереж, реєстрів, форумів тощо), а також вибір інструментів і методів OSINT, які найкраще відповідають поставленим завданням. Грамотне планування дозволяє оптимізувати ресурси та зменшити ризик отримання надлишкової або нерелевантної інформації.

2. Збір інформації з відкритих джерел. На другому етапі здійснюється безпосередній збір даних із загальнодоступних джерел. До таких джерел належать офіційні веб-сайти, соціальні мережі, онлайн-бази даних, публічні реєстри, новинні ресурси, технічні платформи та інші відкриті інформаційні середовища. Для підвищення ефективності збору можуть використовуватися спеціалізовані OSINT-інструменти та фреймворки, зокрема Google Dorks, Shodan, Maltego, SpiderFoot та інші рішення для автоматизованого пошуку й агрегації даних [9, 11, 12, 19, 26]. Застосування таких інструментів дозволяє швидко отримувати великі

обсяги інформації, структурувати її та зменшувати вплив людського фактора.

3. Аналіз, кореляція та верифікація отриманих даних. Після завершення збору інформації ключовим завданням стає її аналіз і перевірка на достовірність. На цьому етапі здійснюється фільтрація отриманих даних, оцінка їх актуальності, релевантності та надійності джерел. Застосовуються методи кореляції інформації з різних джерел, логічного аналізу та встановлення взаємозв'язків між об'єктами дослідження. Верифікація даних є критично важливою складовою OSINT, оскільки відкриті джерела можуть містити помилки, застарілу або навмисно викривлену інформацію. Ретельний аналіз дозволяє мінімізувати ризик хибних висновків та підвищити якість розвідувального продукту [46, 48].

4. Підготовка, оформлення та представлення результатів. Завершальний етап передбачає систематизацію результатів дослідження та підготовку аналітичного звіту. У звіті узагальнюються ключові знахідки, формулюються обґрунтовані висновки та, за потреби, надаються практичні рекомендації. Для підвищення наочності та зрозумілості результатів можуть використовуватися графіки, діаграми, таблиці, часові лінії та інші засоби візуалізації даних. Якісно підготовлений звіт забезпечує ефективну передачу інформації зацікавленим сторонам і сприяє ухваленню обґрунтованих управлінських або оперативних рішень [49,50].

Таким чином, реалізація зазначених етапів формує комплексний підхід до використання можливостей OSINT, що дозволяє ефективно здійснювати збір, аналіз і практичне застосування інформації з відкритих джерел у розвідувальній та кібербезпековій діяльності.

1.6. OSINT методи як превентивні заходи

Методи OSINT (Open Source Intelligence) відіграють важливу роль у реалізації превентивних заходів у сфері інформаційної та кібербезпеки. Їх

застосування дає змогу організаціям і фахівцям з безпеки завчасно виявляти потенційні загрози, прогнозувати можливі вектори атак та мінімізувати ризики, пов’язані з кібератаками, витоком конфіденційної інформації, шахрайством і соціальною інженерією. На відміну від реактивних підходів, OSINT орієнтований на проактивний збір і аналіз інформації, що дозволяє попереджати інциденти ще на етапі їх формування [38,39, 45, 48].

1. Моніторинг соціальних мереж та відкритих веб-ресурсів

Систематичний моніторинг соціальних мереж, форумів, блогів, месенджерів і новинних ресурсів дає змогу виявляти ознаки підготовки атак, витоки інформації, обговорення вразливостей або шкідливі наміри з боку зловмисників. Аналіз відкритих комунікацій дозволяє ідентифікувати потенційні загрози, пов’язані з репутаційними ризиками, фішинговими кампаніями або координованими інформаційними атаками. Використання автоматизованих OSINT-інструментів значно підвищує ефективність такого моніторингу та забезпечує оперативне реагування на підозрілі активності [50-53].

2. Аналіз метаданих і цифрових артефактів

Збір і аналіз метаданих з опублікованих у відкритому доступі документів, зображень і файлів дозволяє виявляти приховану або ненавмисно розкриту службову інформацію. Метадані можуть містити імена співробітників, структуру організації, версії програмного забезпечення, внутрішні шляхи доступу або технічні деталі, що можуть бути використані зловмисниками під час підготовки атаки. Своєчасне виявлення таких даних дає можливість усунути джерела витоку та підвищити рівень інформаційної гігієни в організації [51-54].

3. Виявлення вразливостей і помилок конфігурації

OSINT-методи дозволяють аналізувати відкриту інформацію про мережеву та серверну інфраструктуру з метою виявлення неправильно

налаштованих сервісів, відкритих портів або застарілих компонентів. Такий аналіз дає змогу організаціям виявляти слабкі місця власних систем ще до того, як вони будуть використані зловмисниками. У контексті превентивної безпеки це дозволяє своєчасно усувати технічні недоліки та зменшувати поверхню атаки [55].

4. Аналіз інфраструктури та технологічного стеку

За допомогою OSINT можна отримувати інформацію про використовувані веб-технології, програмні платформи та сервіси, що формують технологічний стек організації. Виявлення застарілих або вразливих технологій дозволяє своєчасно планувати оновлення та впроваджувати додаткові заходи захисту. Такий підхід є особливо ефективним у межах управління ризиками, оскільки дозволяє прогнозувати можливі загрози, пов’язані з експлуатацією відомих вразливостей [52].

5. Збір та аналіз ідентифікаційної інформації

OSINT-методи дають можливість здійснювати аналіз цифрового сліду фізичних осіб і організацій, включаючи доменні імена, електронні адреси, облікові записи в соціальних мережах та інші ідентифікаційні дані. Це дозволяє виявляти спроби підміни особистостей, фейкові акаунти, а також перевіряти достовірність інформації, що використовується у фішингових атаках і соціальній інженерії. Такий аналіз значно підвищує ефективність превентивного захисту від цільових атак [52].

6. Моніторинг даркнету та нелегальних майданчиків

Важливою складовою превентивних заходів є аналіз інформації з даркнету, де часто здійснюється обмін викраденими обліковими даними, фінансовою інформацією та іншими конфіденційними матеріалами. Моніторинг таких ресурсів дозволяє своєчасно виявляти факти компрометації даних і вживати заходів щодо мінімізації наслідків, зокрема зміну паролів, блокування доступів і посилення контролю безпеки [53].

7. Автоматизована оцінка ризиків і безперервний аналіз

Інтеграція OSINT-інструментів із системами управління інформаційною безпекою дозволяє автоматизувати процес збору та аналізу даних, забезпечуючи безперервну оцінку ризиків. Використання автоматизованих платформ і API сприяє своєчасному оновленню інформації про загрози та підвищує здатність організації швидко адаптуватися до змін у кіберзагрозовому середовищі [55].

Таким чином, застосування OSINT-методів як превентивних заходів забезпечує проактивний підхід до захисту інформаційних ресурсів. Вони дозволяють не лише реагувати на інциденти, а й завчасно виявляти та нейтралізовувати потенційні загрози, підвищуючи загальний рівень кібер стійкості організацій.

1.7. OSINT методи як першочергові заходи при виникнення кібератак та загальнодоступні інструменти їх уникнення

Сучасне інформаційне середовище характеризується стрімким зростанням кількості та складності кіберзагроз, серед яких особливе місце займають несанкціоновані втручання в роботу інформаційних систем, витоки даних, фішингові кампанії, шкідливе програмне забезпечення та атаки на критичну інфраструктуру. У таких умовах використання методів Open Source Intelligence (OSINT) набуває особливого значення як на етапі оперативного реагування на інциденти, так і для мінімізації їх наслідків [34, 37, 45, 48]. В Україні питання кібербезпеки регламентується, зокрема, Законом України «Про основні засади забезпечення кібербезпеки України», відповідно до якого інцидент кібербезпеки визначається як подія або сукупність подій, що порушує або може порушити конфіденційність, цілісність чи доступність інформаційних ресурсів та інформаційних систем. У цьому контексті OSINT-методи виступають першочерговим інструментом збору та аналізу інформації, необхідної для своєчасного

реагування на кіберінциденти [43,55,57]. Методи OSINT дозволяють швидко отримувати, аналізувати та систематизувати відкриту інформацію, що є критично важливою на початковому етапі реагування на кібер атаку. Основні напрями їх застосування наведено нижче.

1. Ідентифікація та первинний аналіз загрози. Першочерговим завданням під час виникнення кібератаки є визначення її характеру, джерела та можливих векторів проникнення. OSINT-методи дозволяють оперативно зібрати інформацію про IP-адреси, домени, сервери та сервіси, які можуть бути задіяні в атаці. Аналіз відкритих даних допомагає встановити тип загрози, масштаби ураження та потенційні цілі зловмисників. Для цього використовуються інструменти пошуку вразливих пристроїв, автоматизованого збору інформації про мережеву інфраструктуру та відкриті ресурси організації.

2. Аналіз скомпрометованих і викрадених даних. У разі підозри на витік інформації OSINT дозволяє здійснювати пошук і перевірку даних, які могли бути скомпрометовані або оприлюднені у відкритому доступі. Аналіз таких витоків дає змогу визначити обсяг завданої шкоди, типи викрадених даних та потенційні наслідки для організації. Моніторинг відкритих джерел і нелегальних майданчиків дозволяє своєчасно виявити появу конфіденційної інформації та вжити заходів для її нейтралізації.

3. Виявлення та профілювання зловмисників. OSINT-методи застосовуються для аналізу джерел атаки та встановлення можливих зв’язків між інфраструктурою зловмисників. Дослідження відкритої інформації про сервери, домени, програмне забезпечення та мережеві маршрути дозволяє сформувати базове уявлення про тактику, техніки та процедури атакуючої сторони. Побудова логічних і мережевих зв’язків між об’єктами допомагає виявляти повторювані патерни атак і прогнозувати подальші дії зловмисників.

4. Забезпечення безпеки OSINT-досліджень. Під час проведення OSINT-аналізу важливим аспектом є захист особистих даних і анонімність дослідника. Використання інструментів анонімності дозволяє знизити ризик ідентифікації аналітика та уникнути компрометації його облікових записів або технічних засобів. Забезпечення безпечного середовища дослідження є необхідною умовою ефективного застосування OSINT у кризових ситуаціях.

Загальнодоступні OSINT-інструменти для уникнення кібератак

Значну роль у запобіганні кібератакам відіграють загальнодоступні OSINT-інструменти, які дозволяють виявляти потенційні вразливості ще до їх експлуатації зловмисниками. Серед них варто виокремити інструменти для розширеного пошуку інформації у відкритому доступі, аналізу цифрового сліду користувачів і організацій, визначення технологій, що використовуються на веб-ресурсах, а також вилучення метаданих із загальнодоступних документів. Застосування таких засобів дозволяє своєчасно виявляти ненавмисно оприлюднену конфіденційну інформацію та усувати джерела потенційних витоків.

Рекомендації щодо уникнення кібератак. Для підвищення рівня кіберзахисту доцільно поєднувати OSINT-методи з базовими організаційними та технічними заходами безпеки [56, 59]. Серед основних рекомендацій слід виділити регулярне резервне копіювання даних, своєчасне оновлення програмного забезпечення та встановлення актуальних патчів безпеки, використання багатофакторної автентифікації для захисту облікових записів, а також застосування антивірусних і антишпигунських засобів для виявлення шкідливого програмного забезпечення. Отже, OSINT-методи є не лише інструментом збору відкритої інформації, але й важливою складовою першочергових заходів реагування на кібератаки. Їх комплексне застосування дозволяє оперативно ідентифікувати загрози, зменшити масштаби інцидентів та забезпечити

безперервність функціонування інформаційних систем в умовах зростаючих кібер ризиків.

1.8. Альтернативний профіль для OSINT та інструменти. Алгоритм процесу документування матеріалів. Інструменти для ефективного документування системи.

Ефективне застосування OSINT-досліджень у сучасних умовах потребує використання альтернативного (операційно безпечного) профілю аналітика, а також чітко визначеного алгоритму документування отриманих матеріалів. Альтернативний профіль є сукупністю технічних, інформаційних і поведінкових характеристик, які дозволяють здійснювати збір і аналіз відкритої інформації без розкриття особи дослідника, його справжніх цілей або приналежності до конкретної організації [48-53].

1. Альтернативний профіль OSINT-аналітика. Створення альтернативного профілю є базовим елементом безпеки під час проведення OSINT-досліджень. Такий профіль включає використання окремих облікових записів, спеціалізованих електронних адрес, віртуального середовища, а також інструментів анонімізації мережевого трафіку. Основною метою є мінімізація цифрового сліду аналітика та запобігання його ідентифікації з боку потенційних зловмисників або об’єктів дослідження. Альтернативний профіль дозволяє: безпечно взаємодіяти з відкритими цифровими джерелами; здійснювати моніторинг соціальних мереж і мультимедійного контенту; зменшувати ризик цільових атак у відповідь на OSINT-активність; забезпечувати правдоподібність дослідницької легенди.

Алгоритм процесу документування OSINT-матеріалів. Документування є критично важливим етапом OSINT-дослідження, оскільки забезпечує відтворюваність результатів, перевірку достовірності

та подальший аналітичний аналіз. Процес документування доцільно реалізовувати за таким алгоритмом:

1. **Фіксація джерела інформації** – збереження URL-адрес, часу доступу, типу ресурсу та умов отримання інформації.
2. **Збереження первинного матеріалу** – копіювання фото-, відео- або текстових даних у незмінному вигляді з фіксацією хеш-значень для підтвердження цілісності.
3. **Аналіз і структуризація** – виділення ключових елементів (геолокація, об’єкти, особи, інфраструктура), формування опису та попередніх висновків.
4. **Кореляція даних** – зіставлення матеріалів із іншими відкритими джерелами для підтвердження або спростування отриманої інформації.
5. **Формування аналітичного звіту** – систематизація результатів у вигляді таблиць, схем, таймлайн і текстових висновків.

Чітке дотримання цього алгоритму дозволяє значно підвищити доказову цінність OSINT-матеріалів.

З метою оцінки масштабів проблеми витоку інформації через відкриті цифрові джерела доцільно використовувати низку загальнодоступних інструментів OSINT, які спеціалізуються на аналізі фото-, відео- та геопросторових даних.До ключових інструментів належать:

Google Lens – інструмент візуального пошуку, що дозволяє ідентифікувати об’єкти, написи, місця та схожі зображення.

Google Maps – використовується для визначення координат і аналізу об’єктів інфраструктури, зокрема військових частин, промислових підприємств, об’єктів енергетики та транспортних вузлів.

InVID-We Verify – інструмент для аналізу відеоматеріалів, пошуку оригінальних відео та їх фрагментів через різні пошукові системи.

PimEyes – система пошуку людей за фотографіями, що дозволяє

ідентифікувати цифровий слід особи.

SunCalc та Shadow Map – інструменти аналізу тіней на зображеннях, які дають змогу визначати час зйомки та приблизну геолокацію.

PeakVisor – застосовується для ідентифікації гірського ландшафту на фоні фото або відео з метою географічної прив'язки.

Metadata 2Go – інструмент вилучення метаданих із цифрових зображень, що особливо актуально, оскільки більшість сучасних смартфонів автоматично додають геолокацію.

Geolocation Estimation – нейромережевий інструмент, який намагається визначити місце зйомки за візуальними ознаками зображення.

VGG Image Tools – набір інструментів для пошуку та аналізу зображень, включно з обличчями, об'єктами та технічними елементами.

OpenInfraMap – карта інфраструктурних об'єктів різного призначення в різних країнах світу.

Роль нейромереж у сучасних OSINT-дослідженнях. Основними відкритими цифровими джерелами інформації залишаються фото- та відеоматеріали. Їх аналіз вимагає обробки великих обсягів даних, часто в умовах обмеженого часу. У цьому контексті застосування нейромережевих технологій суттєво полегшує роботу аналітиків. Нейромережі ефективно виконують завдання з: автоматизованого пошуку об'єктів розвідки; розпізнавання осіб і техніки; аналізу зображень і відео; підвищення достовірності отриманої інформації.

Використання таких технологій дозволяє скоротити час на отримання розвідувальних даних, підвищити їх точність і автоматизувати процеси аналізу.

Пошук шляхів удосконалення методів захисту інформації, що розміщується у відкритих джерелах, є перспективним завданням для сил безпеки та оборони України. Зростаючі обсяги відкритих цифрових даних

зумовлюють необхідність створення або посилення спеціалізованих підрозділів, відповідальних за протидію витоку інформації через OSINT-канали. В умовах сьогодення особливої актуальності набуває впровадження OSINT-методів у діяльність Національної гвардії України та організація ефективної взаємодії з іншими складовими сектору безпеки і оборони держави. Це дозволить своєчасно виявляти загрози національній безпеці, підвищити якість розвідувальної інформації та загальний рівень державної безпеки.

1.9. Фреймворк для OSINT. Google Dorks. Розширений пошук. Реверсивний пошук і дослідження зображень. Пошук відео. Метадані

Фреймворк OSINT (Open Source Intelligence) являє собою систематизовану модель організації процесу збору, аналізу, верифікації та документування інформації з відкритих джерел [34-39, 45, 48]. Його основне призначення полягає у забезпеченні комплексного підходу до роботи з великими обсягами відкритих даних, мінімізації часових витрат та підвищенні достовірності отриманих результатів.

OSINT-фреймворк охоплює широкий спектр інструментів і напрямів аналізу, які дозволяють працювати з різними типами інформації — від текстових джерел і мультимедійних матеріалів до технічних даних та цифрових слідів користувачів.

Основні компоненти OSINT-фреймворку [22, 26, 54]

1. Training (Навчання та підготовка). Цей компонент охоплює методичну та практичну підготовку OSINT-аналітиків. Він включає вивчення інструментів, технік збору інформації, правових обмежень, етичних норм, а також формування навичок критичного мислення та аналітичної оцінки джерел.

2. Documentation / Evidence Capture (Документування та фіксація доказів). Документування є ключовим елементом OSINT-фреймворку, що

забезпечує збереження первинних матеріалів у незмінному вигляді. Це включає фіксацію джерел, часових міток, хеш-значень, скріншотів, відео та текстових матеріалів для подальшого аналізу або використання у звітності.

3. OpSec (Operational Security – операційна безпека). OpSec спрямований на захист аналітика та інфраструктури дослідження. Він передбачає використання альтернативних профілів, анонімних середовищ, сегментацію робочих пристроїв, контроль цифрового сліду та запобігання витоку інформації під час OSINT-діяльності.

4. Threat Intelligence (Розвідка загроз). Цей напрям зосереджений на зборі та аналізі інформації про актуальні та потенційні загрози, тактики, техніки й процедури зловмисників. Він використовується для прогнозування атак, виявлення трендів та підтримки превентивних заходів кібербезпеки.

5. Exploits & Advisories (Експлойти та вразливості). Компонент включає аналіз відкритих баз даних уразливостей, звітів виробників програмного забезпечення та експлойтів, що дозволяє своєчасно ідентифікувати технічні ризики та потенційні вектори атак.

6. Malicious File Analysis (Аналіз шкідливих файлів). Цей модуль охоплює попередній аналіз підозрілих файлів із відкритих джерел, зокрема перевірку хешів, метаданих і поведінкових ознак без безпосереднього виконання шкідливого коду.

7. Tools (Інструментальна база). Містить перелік спеціалізованих програмних засобів та онлайн-сервісів, що застосовуються для автоматизації OSINT-процесів: збору, кореляції, аналізу та візуалізації даних.

8. Encoding / Decoding (Кодування та декодування). Цей компонент використовується для аналізу зашифрованих або закодованих даних, що можуть зустрічатися у відкритих джерелах, зокрема у повідомленнях, файлах або прихованих параметрах URL.

Розширені напрямки OSINT-фреймворку

Classifieds, Forums / Blogs / IRC (Аналіз оголошень, форумів, блогів та чатів дозволяє виявляти соціальні, кримінальні або деструктивні активності, а також відстежувати обговорення потенційних загроз). Digital Currency та Dark Web (Охоплює моніторинг криптовалютних операцій та ресурсів даркнету з метою виявлення незаконної діяльності, витоків даних або підготовки атак), Terrorism (зосереджується на аналізі відкритих джерел, пов'язаних із екстремістською діяльністю, радикальними угрупованнями та ін), Mobile Emulation (передбачає аналіз мобільних середовищ, додатків і поведінки користувачів за допомогою емуляції мобільних пристроїв), Metadata (Метадані) (окремий важливий модуль, що охоплює аналіз технічної інформації, прихованої у файлах (EXIF, IPTC, XMP), яка може містити геолокацію, дату створення, модель пристрою та інші чутливі дані), Language Translation (інструменти автоматичного перекладу дозволяють працювати з багатомовними джерелами, розширюючи географічні та інформаційні межі OSINT-досліджень), Archives (робота з веб-архівами дає змогу відновлювати видалений або змінений контент та аналізувати історію змін інформаційних ресурсів).

Пошукові та аналітичні модулі OSINT: Search Engine та Google Dorks (розширений пошук із використанням спеціальних операторів дозволяє виявляти конфіденційну або технічну інформацію, що перебуває у відкритому доступі, але не індексується стандартними запитами), Geolocation Tools / Maps (модуль включає інструменти для просторового аналізу, визначення координат, ідентифікації об'єктів інфраструктури та співставлення географічних даних), Images / Videos / Docs (реверсивний пошук зображень, аналіз відео та документів дозволяє ідентифікувати джерело матеріалу, встановити автентичність контенту та виявити маніпуляції), IP & MAC Address, Domain Name, Email Address, Username (напрям охоплює аналіз технічних ідентифікаторів та цифрових слідів, що

дозволяє встановлювати зв’язки між обліковими записами, доменами, адресами та користувачами),Business Records, Public Records, People Search Engines (аналіз відкритих державних і комерційних реєстрів дозволяє отримувати інформацію про фізичних та юридичних осіб, структуру власності, ділові зв’язки та історію діяльност).

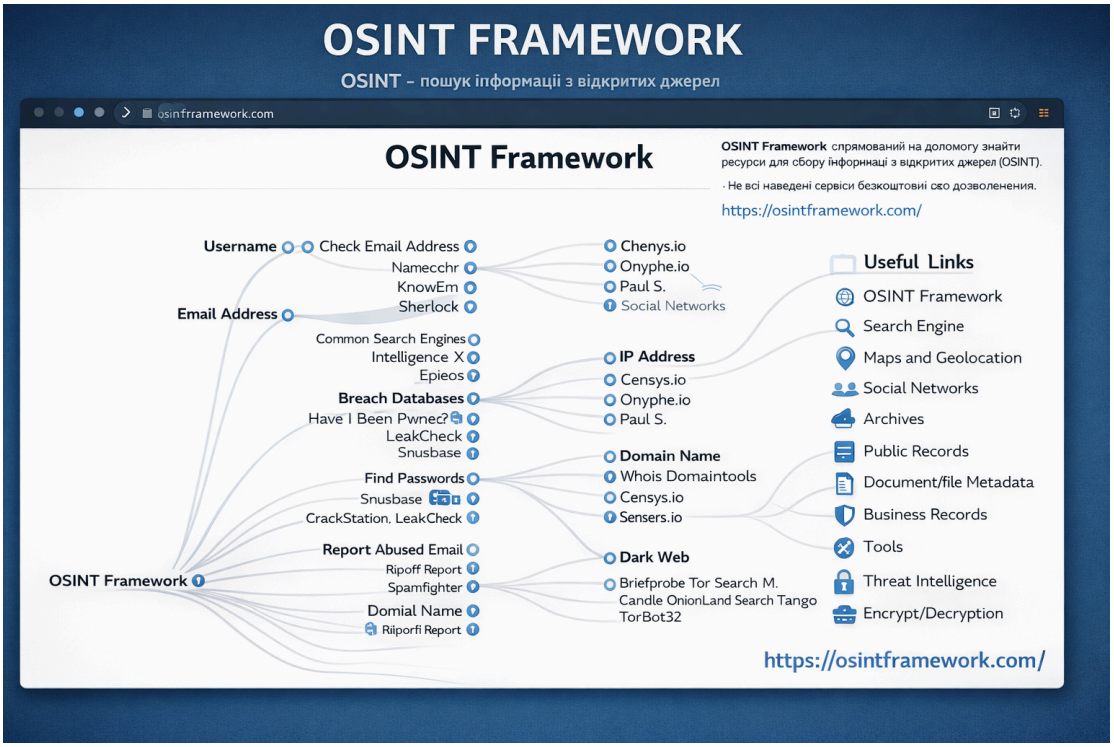


Рис.1.1. Фреймворк для OSINT

Таким чином, OSINT-фреймворк є багаторівневою системою, яка об’єднує інструменти, методи та напрями аналізу в єдину логічну модель. Його застосування дозволяє ефективно організувати процес розвідки з відкритих джерел, підвищити якість аналітичних висновків і забезпечити безпечну та правомірну роботу з інформацією.

Висновки до першого розділу

У результаті проведеного аналізу методів, інструментів і підходів OSINT можна зробити висновок, що розвідка з відкритих джерел є невід’ємною складовою сучасної інформаційної та кібербезпекової діяльності. Застосування спеціалізованих OSINT-інструментів і

фреймворків, зокрема Google Dorks, Shodan, Maltego, SpiderFoot та інших рішень для автоматизованого пошуку й агрегації даних, дає змогу значно підвищити швидкість і повноту збору інформації, забезпечити її структурованість та суттєво зменшити вплив людського фактора на результати дослідження.

Ключовим етапом OSINT-діяльності є аналіз, кореляція та верифікація отриманих даних. Саме на цьому етапі відбувається фільтрація інформаційного шуму, оцінка актуальності й надійності джерел, а також встановлення взаємозв'язків між об'єктами дослідження. Враховуючи те, що відкриті джерела можуть містити застарілу, неповну або навмисно викривлену інформацію, верифікація даних є критично важливою для формування достовірних аналітичних висновків. Застосування кореляційного, логічного та контекстного аналізу дозволяє мінімізувати ризик хибних інтерпретацій і підвищити якість розвідувального продукту.

Завершальним етапом OSINT-дослідження є підготовка, оформлення та представлення результатів. Систематизація зібраної інформації у вигляді аналітичних звітів, доповнених графіками, діаграмами, таблицями та часовими лініями, забезпечує наочність і зрозумілість результатів для зацікавлених сторін. Якісно підготовлений звіт сприяє ефективному ухваленню управлінських, оперативних або стратегічних рішень у сфері безпеки.

Окремо встановлено, що OSINT-методи мають високу цінність як **превентивні заходи**. Проактивний моніторинг соціальних мереж, відкритих веб-ресурсів і даркнету, аналіз метаданих, цифрових артефактів, інфраструктури та технологічного стеку дозволяє завчасно виявляти потенційні загрози, вразливості й ознаки підготовки кібератак. Такий підхід дає можливість зменшити поверхню атаки, усунути

джерела витоку інформації та підвищити загальний рівень кібер стійкості організацій.

OSINT також відіграє важливу роль як **першочерговий інструмент реагування** у разі виникнення кібер інцидентів. Методи аналізу відкритих даних дозволяють оперативно ідентифікувати загрозу, оцінити масштаби витоку або атаки, здійснити первинне профілювання зловмисників і підтримати прийняття рішень щодо мінімізації наслідків інциденту. Водночас ефективність таких заходів значною мірою залежить від дотримання принципів операційної безпеки (OpSec) та використання альтернативного профілю OSINT-аналітика.

У роботі також обґрунтовано важливість чіткого алгоритму документування OSINT-матеріалів. Фіксація джерел, збереження первинних даних, кореляція інформації та формування аналітичних звітів підвищують доказову цінність результатів і забезпечують відтворюваність досліджень. Застосування сучасних інструментів аналізу зображень, відео, метаданих і нейромережевих технологій додатково розширює можливості OSINT та зменшує часові витрати на обробку великих масивів інформації.

Таким чином, OSINT-фреймворк постає як багаторівнева, системна модель, що об’єднує методи, інструменти та процеси в єдину логічну структуру. Його комплексне застосування забезпечує ефективний збір, аналіз, верифікацію та практичне використання інформації з відкритих джерел, підвищуючи рівень інформаційної, кібербезпекової та національної безпеки загалом.

РОЗДІЛ 2. ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ПРИ ПОШУКУ ІНФОРМАЦІЇ З ВІДКРИТИХ ТА ЗАКРИТИХ ДЖЕРЕЛ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ OSINT

2.1. Загальні принципи проєктування систем OSINT

Проєктування OSINT-систем ґрунтується на сукупності принципів, що забезпечують їхню гнучкість, надійність і ефективність у сучасному інформаційному середовищі. До основних принципів належать: **модульність** — система має складатися з окремих компонентів (модулів), які можна легко змінювати, оновлювати або вдосконалювати без порушення роботи всієї системи; **масштабованість** — система повинна бути здатною обробляти зростаючі обсяги даних, підтримувати підключення нових джерел та розширення функціоналу; **безпека** — необхідно забезпечити захист зібраних даних, контроль доступу, а також конфіденційність пошукових запитів і результатів аналізу; **ефективність** — алгоритми збору та обробки інформації мають бути оптимізовані для отримання результатів у мінімальні строки та з раціональним використанням ресурсів; **зручність користування (юзабіліті)** — інтерфейс повинен бути зрозумілим, логічно структурованим і зручним для аналітиків, що підвищує продуктивність і зменшує ймовірність помилок.

2.2. Вибір інструментів та технологій для OSINT

Під час вибору інструментів для OSINT насамперед визначають, з якими типами джерел вони мають працювати, адже саме джерельна база визначає функціональні вимоги до пошуку, збору та аналізу інформації. У практиці OSINT джерела умовно поділяють на відкриті та закриті (обмеженого доступу). До відкритих джерел належать соціальні мережі (Facebook, X/Twitter, LinkedIn, Instagram тощо), новинні сайти, блоги й тематичні форуми, онлайн-каталоги та реєстри компаній (наприклад, OpenCorporates), а також публічні доменні реєстри та технічні дані (WHOIS, DNS-записи). Закриті джерела, своєю чергою, включають захищені бази даних, доступ до яких вимагає авторизації, а також платні сервіси, що надають доступ до архівів інформації або аналітичних звітів.

Відповідно, обраний інструмент повинен забезпечувати доступ до релевантних джерел, підтримувати механізми автентифікації та коректно працювати з обмеженнями доступу, не порушуючи встановлених правил використання таких ресурсів.

Вибір інструментів доцільно здійснювати за сукупністю ключових критеріїв. По-перше, важливими є можливості пошуку: підтримка складних запитів (булеві оператори, фільтри, регулярні вирази), наявність механізмів розширеного пошуку та деталізації результатів, а також здатність до автоматизації збору даних за допомогою скриптів, модулів або планувальників задач. По-друге, суттєве значення мають можливості аналізу: виявлення зв’язків між об’єктами (особами, компаніями, подіями, доменами тощо), кластеризація, статистична обробка та порівняння даних, а також підтримка семантичного й контекстного аналізу. По-третє, важливою є якісна візуалізація результатів, зокрема побудова графів зв’язків і формування звітів у наочному форматі (таблиці, діаграми, графіки) із можливістю збереження результатів для подальшого використання. По-четверте, інструменти мають легко інтегруватися в наявну інфраструктуру організації, що передбачає підтримку REST API для взаємодії з іншими системами, сумісність із поширеними протоколами та форматами (HTTP, JSON, XML), а також можливість підключення до баз даних (SQL/NoSQL) і систем обробки великих даних (наприклад, Elasticsearch або Hadoop).

На практиці в OSINT-дослідженнях часто застосовуються спеціалізовані інструменти, кожен із яких орієнтований на певні задачі. Так, Maltego використовується для побудови й аналізу графів зв’язків між об’єктами; його сильними сторонами є візуалізація складних структур і розширюваність через Transform Hub, а типовими сценаріями — аналіз соціальних мереж, доменів, IP-адрес і організаційних взаємозв’язків. SpiderFoot призначений для автоматизованого збору OSINT-даних [21,24,

26], вирізняється великою кількістю модулів та можливістю локального або хмарного розгортання; його застосовують для сканування ресурсів, оцінки ризиків і пошуку цифрових слідів. Shodan орієнтований на пошук інтернет-пристроїв і сервісів та надає дані про IoT-пристрої, сервери й інші мережеві об’єкти, а також API для автоматизації запитів; типовими сценаріями є аудит безпеки, аналіз експонованих сервісів і відкритих портів. Recon-ng є модульним фреймворком для збору інформації з консольним інтерфейсами та підтримкою автоматизації; його використовують для аналізу доменів, електронних адрес і соціальних профілів. Таким чином, обґрунтований вибір інструментів і технологій має спиратися на типи джерел, вимоги до пошуку й аналізу, можливості інтеграції та специфіку завдань, що вирішуються в межах OSINT-дослідження.

Вибір методів пошуку інформації відіграє ключову роль у якості отриманих результатів. Існує кілька підходів до збору даних, які відрізняються рівнем автоматизації, точністю та швидкістю обробки інформації. У Таблиці 1 наведено обрані основні методи, їхні переваги та недоліки. Вибір методу пошуку залежить від конкретних цілей і вимог користувача. Якщо необхідно отримати точні та перевірені результати, то ручний пошук може бути оптимальним, але при великих обсягах даних автоматизовані системи забезпечують значну економію часу [8,11,12].

Для ефективного збору, обробки та аналізу відкритих даних застосовуються необхідні інструменти, кожен з яких має свої особливості та специфічне призначення.

Таблиця 1. Методи пошуку даних

Метод	Опис	Переваги	Недоліки
Ручний пошук	Пошук інформації безпосередньо користувачем через пошукові системи та бази	Точність; контроль над процесом	Затратно за часом; залежність від навичок користувача

Автоматизовані системи	Використання програм та алгоритмів для збору й аналізу інформації	Швидкість; обробка великих обсягів даних	Потреба в технічних знаннях; ризик отримання нерелевантних даних
Комбіновані методи	Поєднання ручного пошуку й автоматизованих рішень	Гнучкість; ефективність	Вимагає координації; можливі складнощі інтеграції

Вибір конкретного інструмента залежить від типу інформації, яка аналізується, необхідної швидкості обробки даних та рівня технічних навичок користувача. Деякі з них спеціалізуються на візуалізації зв'язків між об'єктами, інші потрібні для пошуку вразливостей у підключених пристроях або глибокому аналізі метаданих. У Таблиці 2 наведено основні інструменти для OSINT-аналізу, їхню функціональність та особливості застосування [8,11,12].

Таблиця 2.
Інструменти для аналізу

Інструмент	Функціональність	Особливості застосування
Maltego	Візуалізація зв'язків між об'єктами, аналіз метаданих.	Висока ефективність у розслідуваннях, складність освоєння для новачків.
Shodan	Пошук інформації про підключені до інтернету пристрої, відкриті порти та вразливості	Необхідність платної підписки для доступу до розширених функцій.
Google Search Operators	Формування складних пошукових запитів із використанням операторів для точного пошуку.	Простий у використанні, ефективний для швидкого пошуку інформації.
Censys	Пошук і аналіз інтернет-активів, таких як сервери чи сертифікати SSL	Потужний інструмент для пошуку вразливостей, але потребує реєстрації.
OSINT Framework	Структурований каталог інструментів для збору інформації	Зручний для початківців, потребує комбінування з іншими платформами.

Spiderfoot	Автоматизація збору даних із соціальних мереж, реєстрів доменів, веб-ресурсів.	Гнучкі налаштування, інтеграція з іншими інструментами.
FOCA	Аналіз метаданих у файлах (документи, зображення тощо).	Зручний для виявлення прихованих даних в документах.
Recon-ng	хмарворк для збору OSINT-даних із різних джерел.	Гнучкість завдяки модульній архітектурі, потребує навичок програмування.

Кожен із запропонованих інструментів для OSINT-аналізу має свої унікальні переваги та недоліки. Maltego є потужним інструментом для візуалізації зв’язків між об’єктами, що робить його незамінним у складних розслідуваннях, але водночас потребує значного часу на освоєння [19]. Shodan та Censys дозволяють швидко отримати інформацію про вразливості в мережах, однак доступ до їхніх повних можливостей часто обмежений платною підпискою [8]. Google Search Operators є ефективним методом для швидкого пошуку конкретної інформації, але вимагає навичок формування запитів [12]. Spiderfoot і Recon-ng [23, 26] забезпечують комплексний збір даних із різних джерел, проте для ефективного використання потребують налаштування та програмних знань. За параметрами точності та швидкодії найефективнішими є спеціалізовані автоматизовані інструменти, такі як Shodan та Spiderfoot [26], тоді як ручний пошук за допомогою Google Search Operators має високу точність, але займає більше часу. Комбіноване використання цих інструментів дозволяє отримати максимально повні результати та підвищити рівень кібербезпеки (Spiderfoot, 2022; Maltego Documentation, 2022; **S**hodan, 2023) [9-12, 17-19, 23, 26]. Загалом, ефективний OSINT-аналіз вимагає вибору інструментів, які найкраще відповідають конкретним цілям та вимогам дослідження.

Крім цих інструментів існує і інші не менш корисні ресурси для розвідки з відкритих джерел інформації [49-53].

Lampyre — це універсальний інструмент для аналізу даних із різних джерел. Він дозволяє проводити розвідку щодо телефонних номерів, IP-адрес, електронних поштових скриньок, соціальних мереж та інших даних. Особливістю є можливість візуалізації отриманої інформації у вигляді графів.

Nmap (Network Mapper) — це популярний інструмент для сканування мережі та виявлення її пристроїв, відкритих портів, версій програмного забезпечення та інших характеристик. Він використовується для оцінки безпеки мережі, пошуку вразливостей і тестування на проникнення.

Creepy — це інструмент для аналізу геолокаційних даних, отриманих із соціальних мереж, публікацій у блогах чи зображень. Creepy використовується для відстеження цифрового сліду особи за допомогою GPS-координат, прив'язаних до її активності онлайн.

Комбінування різних підходів та автоматизованих інструментів, таких як Shodan та Spiderfoot, і більш точного, але часозатратного ручного пошуку за допомогою Google Search Operators – дозволяє забезпечити більш повний і всебічний збір даних. Вибір інструментів також залежить від рівня технічної підготовки аналітика та необхідності оперативного отримання інформації [12]. Використання таких інструментів у комплексі може значно підвищити ефективність розслідувань і забезпечити високий рівень кібербезпеки, мінімізуючи ймовірність пропущених загроз чи вразливостей.

2.3. Архітектура системи пошуку інформації

Архітектура системи OSINT (Open Source Intelligence) формується як багаторівнева структура, що об'єднує низку взаємопов'язаних компонентів,

кожен з яких виконує визначену функцію у процесі збору, обробки, аналізу та представлення інформації. Такий підхід дозволяє забезпечити логічну послідовність роботи з даними, підвищити ефективність аналітичних процесів і спростити подальший розвиток системи [34,36, 37, 48]..

Центральним елементом архітектури є **модуль збору даних**, який відповідає за отримання інформації з відкритих, а за наявності відповідних прав доступу — і з обмежених джерел. У межах цього модуля використовуються інструменти веб-сканування, зокрема бот-системи, парсери та краулери, що автоматизовано здійснюють збір даних із веб-сайтів, блогів, форумів та інших онлайн-ресурсів. Важливу роль відіграє використання офіційних і неофіційних API соціальних мереж для отримання інформації з таких платформ, як Twitter, Facebook, LinkedIn, Instagram тощо. Окремий напрям становлять системи роботи з Dark Web, які забезпечують збір даних з анонімних мереж, зокрема мережі Tor. Крім того, модуль збору даних передбачає підключення до зовнішніх публічних баз даних, реєстрів, пошукових систем та онлайн-архівів.

Наступним ключовим компонентом є **модуль обробки даних**, призначений для підготовки зібраної інформації до аналітичної обробки. На цьому етапі реалізуються алгоритми очищення даних, які спрямовані на видалення дублікатів, інформаційного шуму та нерелевантних записів. Подальша класифікація даних здійснюється за тематикою, ключовими словами або метаданими, що дозволяє структурувати інформацію та спростити її аналіз. Важливою функцією модуля є фільтрація, яка забезпечує відбір лише тих даних, що відповідають заданим критеріям пошуку. Підготовлені дані зберігаються у структурованих форматах, зокрема у реляційних і нереляційних базах даних (SQL, NoSQL), а також в індексованих сховищах для швидкого доступу.

Модуль аналізу забезпечує безпосередню інтерпретацію даних і формування аналітичних висновків. Він включає інструменти для побудови

звітів, проведення статистичного аналізу та застосування методів машинного навчання з метою прогнозування та виявлення прихованих закономірностей. Значне місце в межах цього модуля займає геолокаційний аналіз, який дозволяє визначати географічне розташування об’єктів на основі зібраної інформації. Для наочного представлення результатів використовуються засоби візуалізації у вигляді графіків, діаграм і мережевих графів, що ілюструють взаємозв’язки між даними. Додатково застосовуються методи семантичного аналізу, спрямовані на виділення ключових понять, сутностей і контексту в текстових масивах інформації.

Взаємодію користувача з системою забезпечує **інтерфейс користувача**, який надає зручний доступ до функціональних можливостей OSINT-системи. Через панель керування користувачі можуть формувати пошукові запити, налаштовувати параметри збору даних та переглядати результати аналізу. Система сповіщень дозволяє отримувати повідомлення або оновлення за заздалегідь визначеними критеріями, що підвищує оперативність реагування. Адаптивний інтерфейс забезпечує коректну роботу системи на різних пристроях, зокрема на персональних комп’ютерах і смартфонах.

Окрім основних компонентів, архітектура OSINT-системи може містити **додаткові модулі**, які розширюють її функціональні можливості. До них належать модуль безпеки, що відповідає за шифрування даних, управління доступом і виявлення аномалій, модуль інтеграції для взаємодії з іншими інформаційними системами через API, а також модуль навчання, який включає бази знань і рекомендаційні механізми для автоматичного вдосконалення пошукових і аналітичних процесів.

Загалом архітектура OSINT-системи має бути гнучкою та масштабованою, щоб відповідати потребам аналітиків, специфіці поставлених завдань і динаміці сучасного інформаційного середовища.

2.4. Етапи проєктування OSINT-системи

Проєктування OSINT-системи є поетапним процесом, який охоплює послідовні організаційні, технічні та аналітичні дії, спрямовані на створення ефективного, надійного й адаптивного інструменту роботи з відкритими та обмежено доступними джерелами інформації. Чітке дотримання етапів проєктування дозволяє зменшити ризики помилок, оптимізувати витрати ресурсів і забезпечити відповідність системи поставленим вимогам.

Першим етапом є **визначення вимог до системи**. На цьому кроці здійснюється детальний аналіз завдань, які має вирішувати OSINT-система, зокрема збір даних, їх обробка, аналіз, візуалізація та формування звітів. Важливим елементом є ідентифікація користувачів і визначення цільової аудиторії системи, якою можуть бути аналітики з кібербезпеки, представники правоохоронних органів, фахівці приватних компаній або дослідники. Паралельно проводиться оцінка потенційних джерел даних, таких як веб-сайти, соціальні мережі, публічні реєстри, API та онлайн-архіви. На основі цього формуються функціональні вимоги (перелік конкретних можливостей системи, наприклад, пошук за ключовими словами, підтримка багатомовності, автоматизований збір даних) і нефункціональні вимоги, які охоплюють продуктивність, масштабованість, безпеку, зручність інтерфейсу та надійність роботи.

Другим етапом є **розробка концептуальної моделі OSINT-системи**. На цьому етапі визначається загальна архітектура системи та логіка взаємодії її основних компонентів: модулів збору, обробки, аналізу даних і користувацького інтерфейсу. Здійснюється вибір технологій, програмних інструментів і платформ, які доцільно використовувати для реалізації кожного модуля. Для наочного представлення процесів будуються схеми та діаграми, зокрема UML-діаграми, що відображають потоки даних і взаємодію компонентів. Окремо визначаються протоколи та стандарти

взаємодії між модулями, включно з використанням REST API, форматів обміну даними, механізмів автентифікації та шифрування.

Третій етап передбачає **тестування концепції**. Його метою є перевірка життєздатності обраних рішень ще до повномасштабної реалізації системи. На цьому кроці тестуються окремі компоненти, наприклад ефективність веб-сканування або коректність обробки даних із соціальних мереж. Для цього використовуються наявні тестові набори даних або обмежені реальні дані. Проводиться аналіз коректності результатів, зокрема оцінюється, чи відповідає отримана інформація очікуванням користувачів і поставленим цілям. За підсумками тестування вносяться корективи до концептуальної моделі.

Наступним етапом є **імплементація та інтеграція системи**. Вона починається зі створення прототипу (MVP), у межах якого реалізується базовий функціонал OSINT-системи для практичного тестування. Далі відбувається об’єднання модулів збору, обробки та аналізу даних у єдину систему, розробка користувацького інтерфейсу з можливістю адаптації до різних платформ і налаштування механізмів автоматизованого збору та обробки інформації. Після цього проводиться комплексна перевірка системи на відповідність початковим вимогам і оцінюється її продуктивність у різних режимах роботи.

Завершальним етапом є **комплексне тестування та оптимізація**. Система перевіряється на великих обсягах даних і за різноманітних сценаріїв використання, що дозволяє виявити вузькі місця та потенційні проблеми. Важливим елементом цього етапу є отримання зворотного зв’язку від потенційних користувачів, на основі якого здійснюється виправлення виявлених помилок і подальша оптимізація функціональності.

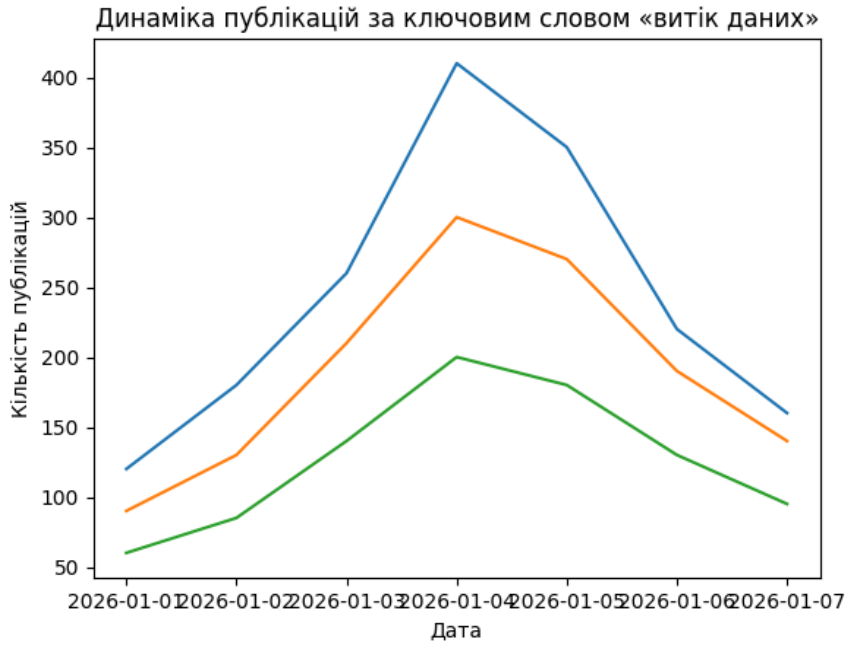
Як приклад можна розглянути проєктування OSINT-системи для моніторингу інформаційних загроз у соціальних мережах. На етапі визначення вимог було встановлено, що система має автоматично збирати

публічні дописи та коментарі з платформи X (Twitter), Facebook та Instagram за визначеними ключовими словами, хештегами та тематичними маркерами. Зібрана інформація підлягає подальшому аналізу з метою визначення тональності повідомлень, інтенсивності поширення контенту та, за можливості, географічної прив’язки публікацій.

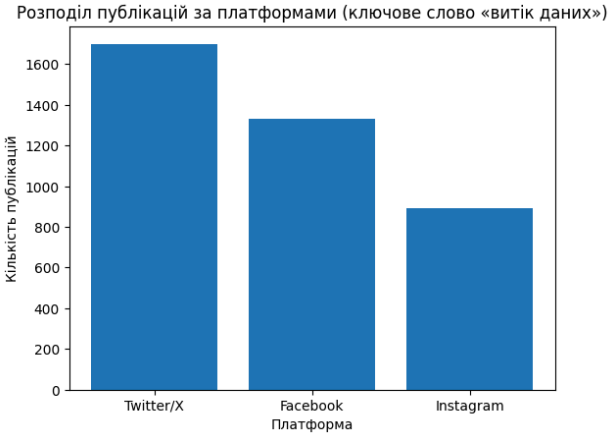
Концептуальна модель системи передбачала використання офіційних API соціальних мереж (у межах дозволеного функціоналу), бази даних **Elasticsearch** для зберігання та швидкого пошуку інформації, а також аналітичного модуля для обробки текстових і метаданих. Для представлення результатів аналізу було передбачено модуль візуалізації у вигляді графіків і діаграм, що дозволяють наочно відображати динаміку інформаційних загроз у часі.

Під час тестування концепції було виявлено, що значна частина публікацій в Instagram не містить явних геолокаційних даних. У зв’язку з цим було прийнято рішення доповнити систему алгоритмами контекстного аналізу тексту, аналізу хештегів і візуального контенту (зображень), що дозволило частково компенсувати відсутність прямих координат.

Для візуалізації результатів роботи OSINT-системи було побудовано **графік динаміки публікацій за ключовими словами у соціальних мережах**. По осі абсцис відкладено часові інтервали (дні або години), а по осі ординат — кількість зафіксованих публікацій. Окремими лініями графіка відображено активність для кожної платформи (X/Twitter, Facebook, Instagram), що дозволяє порівнювати інтенсивність поширення інформації між різними джерелами. Такий графік наочно демонструє пікові періоди інформаційної активності, дає змогу виявляти аномальні сплески публікацій і може використовуватися аналітиками для своєчасного реагування на потенційні інформаційні загрози.



а)



б)

в)

Рисунок 2.5. а) Динаміка публікацій за ключовим словом -витік даних б) розподіл публікацій за платформами, в)тональність публікацій за ключовим словом

2.5. Розробка алгоритмів пошуку та аналізу інформації для OSINT-систем

Розробка алгоритмів пошуку та аналізу інформації є одним із ключових факторів ефективності OSINT-систем, оскільки саме алгоритмічні рішення визначають швидкість отримання даних, їхню

релевантність та аналітичну цінність. Алгоритми OSINT повинні враховувати як різноманітність типів даних, так і специфіку джерел, з яких ці дані надходять.

1. Алгоритми обробки даних за їх типами

Алгоритми пошуку та аналізу в OSINT-системах адаптуються залежно від типу інформації. Для текстових даних застосовуються алгоритми пошуку за ключовими словами, фразами та регулярними виразами, а також аналіз метаданих (дата створення, авторство, джерело). Текстова інформація проходить етап нормалізації, що включає очищення від зайвих символів, приведення до нижнього регістру, токенізацію та лематизацію.

Для зображень використовуються технології комп'ютерного зору, зокрема OCR для розпізнавання тексту, алгоритми класифікації об'єктів, аналіз EXIF-метаданих з метою визначення часу створення, геолокації та джерела зображення, а також пошук за візуальною схожістю (reverse image search).

Відеодані аналізуються шляхом розпізнавання об'єктів і сцен у кадрах, вилучення аудіодоріжки з подальшим перетворенням мовлення в текст, а також аналізу технічних метаданих (формат, тривалість, джерело).

Для структурованих даних (таблиці, бази даних, графи) застосовується аналіз атрибутів, пошук закономірностей і виявлення взаємозв'язків між об'єктами, що особливо важливо для побудови аналітичних моделей і графів зв'язків.

2. Стратегії пошуку та збору інформації

Для підвищення ефективності збору інформації алгоритми OSINT підтримують різні стратегії пошуку. Основною є робота з ключовими словами із застосуванням логічних операторів AND, OR, NOT, а також методів стемінгу й лематизації. У соціальних мережах широко використовується аналіз хештегів і взаємодій користувачів для визначення контексту та популярності тем.

Важливу роль відіграє використання метаданих, зокрема геолокації, часу публікації та авторства, що дозволяє фільтрувати результати й підвищувати їхню релевантність. Для розширеного пошуку застосовуються API пошукових систем (наприклад, Google Custom Search API), а також спеціалізовані запити до індексованих веб-ресурсів і, за наявності правових підстав, до сегментів Dark Web.

Узагальнений потік обробки інформації в OSINT-системі має такий вигляд:

ідентифікація джерел → збір даних → фільтрація → нормалізація → лінгвістичний або візуальний аналіз → кореляція → візуалізація результатів.

2.5.1. Приклад практичного застосування алгоритмів (моніторинг підозрілих вакансій)

Як конкретний приклад розглянуто моніторинг підозрілих вакансій на платформі LinkedIn для перевірки фішингових кампаній [64]. Для розв’язання задачі використано представлений алгоритм аналізу даних (Лістинг 2.5.1.1.). Для початку виконували збір даних за допомогою API LinkedIn для пошуку вакансій за ключовими словами: “remote job”, “work from home”, використовуючи ручний пошук, аналітичні інструменти, Python, бібліотеки requests і BeautifulSoup для збору інформації. Парсинг результатів пошуку показав збір описів вакансій, контактних даних, посилань на компанії. Як альтернативу було взято автоматизований пошук за допомогою специфічних запитів, наприклад: site:linkedin.com/jobs “remote job” “apply now”, – тому відповідно отримано велику кількість даних про вакансії, включаючи посилання, опис, компанії та контактні дані. Приклад з пошуку інформації про вакансії в соціальних мережах показав, що автоматизація збору даних із використанням API та пошукових операторів значно прискорює процес отримання релевантної інформації,

при цьому використання специфічних пошукових платформ та індексованих веб-ресурсів забезпечує ефективний доступ до великих масивів даних.

```
import networkx as nx
import matplotlib.pyplot as plt
from googlesearch import search

# Завдання 1: Збір інформації з відкритих джерел
query = "cybersecurity job postings site:linkedin.com"
results = []
for result in search(query, num_results=10):  # Збираємо перші 10 результатів
    results.append(result)

# Завдання 2: Фільтрація шуму (відбір лише релевантних URL)
filtered_results = [url for url in results if "linkedin.com" in url]

# Завдання 3: Створення графів зв'язків
G = nx.Graph()

# Додавання вузлів та зв’язків
for idx, url in enumerate(filtered_results):
    G.add_node(url, label=f"Job {idx+1}")
    G.add_edge("Cyber Security Jobs", url)

# Візуалізація графа
plt.figure(figsize=(10, 8))
pos = nx.spring_layout(G)
nx.draw(G, pos, with_labels=True, node_color='lightblue', font_size=10,
node_size=3000, font_weight='bold')
plt.title("Graph of Job Postings and Relationships")
plt.show()
```

Лістинг 2.5.1.1. Аналіз даних (Python)

Аналіз даних за допомогою Python показав задані пошукові запити, фільтрацію та побудову графів зв’язків. При цьому використовуючи google search для автоматизованого збору URL за даним запитом, фільтрувалися лише URL, що належать до linkedin.com, для того, щоб залишити лише релевантні результати [12]. Далі було створено граф, де вузли представляють вакансії, а зв’язки ілюструють взаємозв’язки. Алгоритмічна обробка даних для фільтрації шуму, контекстного аналізу та перехресної перевірки, показана на Рисунку 3, включає фільтрацію, що спрямована на видалення нерелевантної або зайвої інформації з отриманих даних. Для цього зроблено попереднє очищення даних, тобто видалення дублікатів, фільтрація за ключовими словами-фразами та виявлення та усунення спаму, реклами чи шкідливого контенту. Для застосування регулярних

виразів для пошуку специфічних патернів у текстах (наприклад, IP-адрес, email-адрес) та використання бібліотек обробки тексту, таких як NLTK, Spacy, прокласифіковано контент за допомогою моделей машинного навчання для визначення релевантності.

Рисунок 2.5.1.2. Алгоритм фільтрації шумів

Наступний етап полягав у контекстному аналізі, зокрема він дозволив оцінити зміст отриманих даних та визначити їхню відповідність поставленим завданням. Методами NLP була токенізація та лематизація тексту для уніфікації форм слів, аналіз тональності текстів (Sentiment Analysis) для розуміння емоційного забарвлення інформації, використання графів зв’язків для встановлення взаємозв’язків між об’єктами даних, визначення ключових об’єктів та понять у текстах. Крім того, важливим була оцінка джерела за репутацією та надійністю джерел інформації за допомогою рейтингових систем або історичних даних. В подальшому провели перехресну перевірку даних, що забезпечило підвищення точності результатів шляхом порівняння даних із різних джерел, використовуючи крос-перевірку за допомогою різних платформ (наприклад, пошук згадок у соціальних мережах, форумах, офіційних реєстрах) та пошук підтверджень через незалежні джерела.

За рахунок використання API для збору інформації з декількох платформ та автоматичного порівняння отриманих результатів з використанням бібліотек аналізу даних, таких як Pandas або NumPy, виявлено невідповідності між даними за допомогою кластеризації та моделей аномалій. За рахунок даних методів досягнуто скорочення обсягу

оброблюваної інформації та отримано підвищення релевантності даних. Аналогічно визначено ключові теми та їхню значущість, покращено інтерпретацію текстів для стратегічних цілей. Власне, таким чином забезпечено ефективну обробку інформації для ухвалення рішень в умовах кіберзагроз.

У представленому прикладі фільтрували шум, використовуючи NLP для видалення нерелевантних вакансій, тобто видалили записи, що не містять контактні дані або містять підозрілі шаблони тексту («*ми забезпечимо ваше навчання безкоштовно, але треба внести оплату*»). Крім того, провели контекстний аналіз, зокрема аналіз опису вакансій на наявність ключових фраз, таких як: «*немає досвіду? це не проблема»* або *лише через цей сайт»* та виділили підозрілі контактні дані: електронна пошта із загальнодоступних доменів (*gmail.com*, *yahoo.com*). Далі провели перехресну перевірку через зіставлення зібраної інформації з базами даних відомих компаній, щоб визначити фейкові профілі. Як результат, було виділено релевантну інформацію, що свідчила про можливу шахрайську діяльність [64].

У процесі роботи було виконано виділення релевантної інформації за допомогою алгоритмів фільтрації, що усувають нерелевантні дані, такі як дублікати, неактуальні пости або рекламні матеріали. Контекстний аналіз та перехресна перевірка, наприклад, звірка електронних адрес та IP-адрес, додало точність і достовірність отриманих результатів. Графи зв’язків є ефективним методом для аналізу складних взаємозв’язків між різними об’єктами у контексті кіберзагроз. Вони візуалізують та ідентифікують структури, залежності та поведінкові моделі потенційних атак.

На етапі збирання інформації про об’єкти загроз використано різноманітні джерела даних, які допомогли сформувати повну картину потенційних загроз. Зокрема, IP-адреси публічно доступні дані про мережеві з’єднання та вразливості, зокрема через інструменти на кшталт

Shodan чи Censys [8], дозволив виявити відкриті порти та потенційні вразливості в мережах. Домени, тобто використання даних WHOIS та інших реєстраційних баз даних для ідентифікації власників доменів, а також пошук історичних даних, які вказували на зв’язки з потенційно небезпечними об’єктами. Email-адреси збирали інформації з відкритих джерел, таких як соціальні мережі, форуми, чи спеціалізовані сервіси для перевірки email-адрес на наявність у базах даних, що містять виведені в мережу дані. Аналіз профілів у соціальних мережах, форумах, а також перевірка облікових записів на предмет можливих загроз або аномальних активностей та збір метаданих файлів, аналіз шкідливих програм чи іншої компрометуючої інформації через відкриті джерела, такі як репозитарії файлів, бази даних загроз або спеціалізовані інструменти, як VirusTotal передбачили використання публічно доступних даних для збору, аналізу та виведення висновків про потенційні загрози, а також для виявлення зв’язків між об’єктами загрози (Таблиця 3).

Таблиця 3.

Моніторинг підозрілих вакансій на платформі LinkedIn

Запит для збору даних та ключові слова	Шум та фільтрація нерелевантних даних	Алгоритмічна обробка даних для фільтрації шуму, контекстний аналіз та перехресна перевірка	Потенційні загрози
API LinkedIn: “remote job” (“remote job”, “remote”, “work from home”)	Вакансії без згадки про віддалену роботу, фальшиві вакансії	Використання алгоритмів для видалення пошукового шуму (фільтрація за частотою слів, NLP для розпізнавання неактуальних оголошень); перевірка вакансії через кілька платформ (LinkedIn, Glassdoor, Indeed) для виявлення аномалій.	Потенційні фішингові кампанії, шахрайство з оплатою, надання фальшивої інформації для збору особистих даних або грошей.
API LinkedIn: “work from home” (“work from home”, “home office”,	Вакансії, де згадується лише офісна робота	Використання алгоритмів класифікації текстів для виявлення несумісних описів вакансій; перевірка вакансії на наявність термінів, що підтверджують віддалену	Збори даних для фішингових кампаній, використання вакансій для збору адрес електронної

“telecommute ”)		роботу, порівняння опису з іншими джерелами.	пошти та персональних даних.
Ручний пошук: “remote job” (“remote job”, “virtual”, “home-based”)	Реклама на вакансії без конкретної інформації	Використання текстових класифікаторів для автоматичної перевірки вакансій, що не містять точних відомостей про віддалену роботу; перевірка контексту вакансії на основі фраз, що вказують на віддалений характер роботи.	Шахрайство з передоплатами, використання недійсних компаній або пустих вакансій для збору особистої інформації.
Ручний пошук: “work from home” (“work from home”, “work at home”)	Вакансії без опису "віддалено" або що вимагають переїзду	Алгоритм автоматичної фільтрації вакансій, що не містять термінів "work from home" у описах, перевірка вакансій на коректність опису умов роботи з дому.	Невірні або фальшиві вакансії, що призводять до витоку особистої інформації або фінансових втрат через шахрайські сайти.
API LinkedIn: “remote job” + “security” (“remote job”, “security”, “cyber security”)	Реклами вакансій, що не відповідають запиту (шум)	Виявлення помилкових вакансій за допомогою аналізу специфічних термінів галузі (наприклад, “security” в контексті вакансій); перевірка вакансій на спеціалізованих сайтах безпеки для підтвердження наявності вакансії в реальних компаніях.	Потенційні загрози фішингових атак, зловмисне використання вакансій для збору інформації про користувачів або здійснення кібернападів.

Аналіз Таблиці 3 показав, що ефективний моніторинг вакансій на LinkedIn потребує комплексного підходу, який включає використання алгоритмічних методів для фільтрації шуму та перевірки релевантності даних, зокрема через порівняння вакансій з іншими платформами. Алгоритмічна обробка даних, зокрема текстовий аналіз, дозволяє значно зменшити кількість нерелевантних вакансій та покращити точність визначення потенційних загроз, таких як фішингові кампанії або шахрайські оголошення. Перехресна перевірка вакансій із кількох джерел підвищує надійність результатів і дозволяє виявити фальшиві або ненадійні

вакансії, що можуть спричинити фінансові або інформаційні ризики для користувачів.

Наступним було сформовано структуру графа, де вершини: кожен об’єкт (загроза, IP-адреса, користувач); ребра: взаємозв’язки між об’єктами (спільні IP, схожі домени, перехресні активності), між якими виділено прямі та непрямі взаємозв’язки. При обробці даних відфільтровано нерелевантні об’єкти (за допомогою алгоритмів фільтрації шуму) та класифіковано за рівнем загрози (використання рейтингів ризику чи індексів довіри). При візуалізація графа використані інструменти для побудови графів (Gephi, Cytoscape, Neo4j) та накладено шари даних (геолокація, час активності, типи атак). Для аналізу графів визначено алгоритм центральності (Degree, Betweenness, Closeness) для визначення ключових об’єктів та ідентифіковано найбільш активні або ризиковані вузли у мережі. Граф показав зв’язки між зараженими пристроями та командними серверами та дозволив встановити спільні оператори за доменами та email-адресами. Побудова такого графа допомогла зрозуміти структуру загроз, швидко виявила критичні взаємозв’язки та провела ефективне розслідування.

Щодо прикладу про вакансії в соціальних мережах виконано побудову графа зв’язків з допомогою Python-бібліотеки (*networkx*). Для графів позначено вершини: вакансії, контактні дані, IP-адреси, компанії, електронні адреси, ребра: взаємозв’язки між вакансіями (спільні контактні дані, IP). При аналізі виявлено вузли, що часто повторюються (наприклад, один і той самий email у різних вакансіях) та зроблено групування вакансій за спільними атрибутами. З допомогою представлено графу на Рисунку 3 продемонстровано структуру взаємозв’язків між підозрілими вакансіями, що дозволило визначити джерело кіберзагрози.

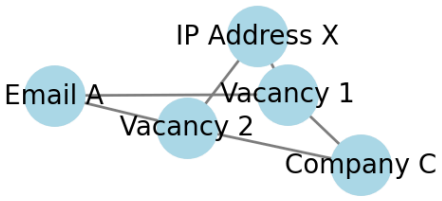


Рисунок 2.5.1. 3. Граф вакансій в соціальних мережах

На графі зв'язків представлено, як взаємопов'язані об'єкти (наприклад, вакансії, контактні дані, IP-адреси) можуть допомогти зрозуміти структуру потенційних загроз. Такий підхід сприяв виявленню прихованих зв'язків між різними елементами, що дозволяє ефективніше аналізувати інформацію і приймати зважені рішення. В результаті отримали ефективну систему збору даних із відкритих джерел, зменшення часу пошуку та аналізу інформації, підвищення точності та релевантності отриманих результатів [64].

2.5.2. Приклад практичного застосування алгоритмів(виявлення витоку даних і фішингових кампаній електронної пошти)

В OSINT-системах доцільно розглянути на прикладі виявлення витоку даних і фішингових кампаній, що здійснюються через електронну пошту. Подібні інциденти є одними з найпоширеніших кіберзагроз і часто супроводжуються появою відкритих слідів у публічному інформаційному просторі [59, 60, 64]. На етапі **збору даних** було сформовано пошукові запити з використанням ключових слів і фраз, пов'язаних із витоками інформації, зокрема *"data breach"*, *"leaked database"*, *"password dump"*, *"phishing email"*, *"credentials leak"*. Збір інформації здійснювався з відкритих джерел за допомогою пошукових операторів Google, спеціалізованих форумів, соціальних мереж, публічних репозиторіїв, а також сервісів моніторингу витоків даних. Для автоматизації процесу використовувалися програмні засоби на базі Python із застосуванням бібліотек requests, BeautifulSoup та pandas, що дозволило зібрати

URL-адреси, фрагменти текстів, списки електронних адрес і посилання на скомпрометовані ресурси. Після збору інформації було виконано алгоритмічну фільтрацію шуму, спрямовану на видалення дублікатів, рекламного контенту та нерелевантних матеріалів. Фільтрація здійснювалася за допомогою регулярних виразів для виявлення електронних адрес, доменів та IP-адрес, а також за частотним аналізом ключових слів. На цьому етапі значну роль відіграли методи обробки природної мови (NLP), зокрема токенізація та лематизація текстів, що дозволило уніфікувати різні форми слів і підвищити точність подальшого аналізу.

Наступним кроком став **контекстний аналіз зібраних даних,** який дозволив оцінити характер повідомлень і виявити ознаки фішингових кампаній. До таких ознак належали типові шаблони фішингових листів, зокрема фрази на кшталт *«терміново підтвердьте обліковий запис»*, *«ваш акаунт буде заблоковано»*, *«перейдіть за посиланням для оновлення пароля»*. Додатково проаналізовано доменні імена відправників, що часто імітували відомі бренди, але мали незначні відхилення в написанні, а також використання загальнодоступних поштових доменів для масових розсилок.

Для підвищення достовірності результатів було проведено перехресну перевірку даних шляхом порівняння зібраної інформації з кількох незалежних джерел. Зокрема, електронні адреси та домени перевірялися через відкриті бази витоків даних, публічні реєстри доменів (WHOIS) та сервіси перевірки компрометації облікових записів. Застосування бібліотек NumPy і pandas дало змогу виявити аномалії та невідповідності у даних, а також кластеризувати повідомлення за схожими ознаками.

Окрему увагу було приділено графовому аналізу, який може візуалізувати взаємозв’язки між об’єктами загрози. У побудованому графі вершинами виступали електронні адреси, домени, IP-адреси та фрагменти фішингових повідомлень, а ребрами — взаємозв’язки між ними (спільні

домени, однакові сервери розсилки, повторювані шаблони текстів). Аналіз центральності вузлів дав змогу визначити ключові елементи інфраструктури фішингової кампанії, зокрема основні домени-ретранслятори та адреси керування.

У результаті застосування алгоритмів фільтрації, контекстного аналізу, перехресної перевірки та графового моделювання було виділено релевантні ознаки витоку даних і фішингових атак. Запропонований підхід дозволив суттєво скоротити обсяг інформації, що підлягає ручному аналізу, підвищити точність виявлення загроз і забезпечити формування обґрунтованих аналітичних висновків. Таким чином, OSINT-алгоритми довели свою ефективність як інструмент первинного виявлення кібер інцидентів і підтримки прийняття рішень у сфері інформаційної безпеки (таблиця 4).

Застосування OSINT дозволяє виявляти фішингові кампанії як на етапі підготовки (аналіз доменів, шаблонів), так і після інциденту (моніторинг витоків, повторюваних email-адрес і серверів)(рисунок 2.5.2.1,2.5.2.2)

Підготовка атаки
↓
Збір даних про жертву (OSINT) (соцмережі, email, витоки, профілі)
↓
Створення фішингового повідомлення (підроблений бренд, домен, шаблон)
↓
Розсилка листів / повідомлень (email, месенджери, соцмережі)
↓
Взаємодія жертви (перехід за посиланням / вкладення)
↓
Компрометація даних (викрадення логінів, паролів, даних)
↓
Витік або продаж інформації (форуми, Dark Web, бази витоків)
↓
OSINT-моніторинг та виявлення (аналіз доменів, email, текстів, графів)

Рис.2.5.2.1. Алгоритм фішингової атаки та її виявлення засобами OSINT

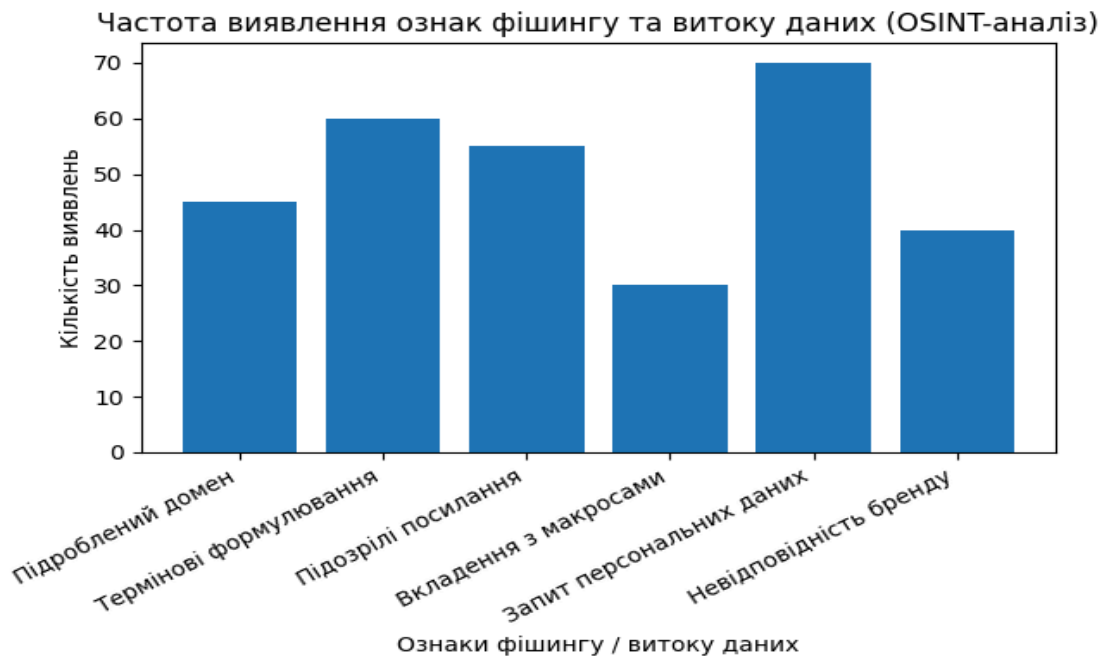


Рис.2.5.2.2.Частота виникнення фішингу та витоку даних

Таблиця 4

Ознаки фішингу та витоку даних

Ознака	Опис	OSINT-методи виявлення	Потенційна загроза
Підроблений домен	Домен імітує бренд (g00gle.com, paypa1.com)	WHOIS, DNS, Google Dorks	Крадіжка облікових даних
Термінові формулювання	«Терміново підтвердити акаунт»	NLP, аналіз тексту	Соціальна інженерія
Підозрілі посилання	Скорочені або приховані URL	URL-аналіз, sandbox	Перенаправлення на фішинг
Вкладення з макросами	Документи з шкідливим кодом	Аналіз вкладень, VirusTotal	Інфікування системи
Запит персональних даних	Логіни, паролі, коди доступу	Контент-аналіз	Витік конфіденційної інформації

Невідповідність бренду	Логотипи й текст неузгоджені	Візуальний аналіз, reverse image search	Фейкові кам

2.6. Практичні приклади OSINT-пошуку за цифровими артефактами

У практиці кіберрозвідки OSINT-аналіз часто починається не з “абстрактної теми”, а з конкретного артефакта: **email**, **нікнейм**, **URL**, **зображення**, **IP**, **адреса крипто гаманця**, **відеоконтент**. Нижче наведені типові сценарії, алгоритми дій та інструменти, які дозволяють швидко зібрати доказову базу, зменшити невизначеність і виявити зв’язки між об’єктами.

2.6.1. Пошук інформації за деталями електронного листа

В умовах зростання кіберзагроз аналіз електронного листа є одним із найрезультативніших напрямів OSINT, оскільки саме email зазвичай містить концентрований набір технічних і змістових маркерів, придатних для швидкої первинної атрибуції інциденту. До таких маркерів належать службові заголовки повідомлення (headers), домен і адреса відправника, IP-адреси серверів на маршруті доставки, посилання, вкладення, а також поведінкові ознаки, характерні для соціальної інженерії (штучна терміновість, підміна бренду, вимога підтвердити доступ або “негайно” оновити дані).

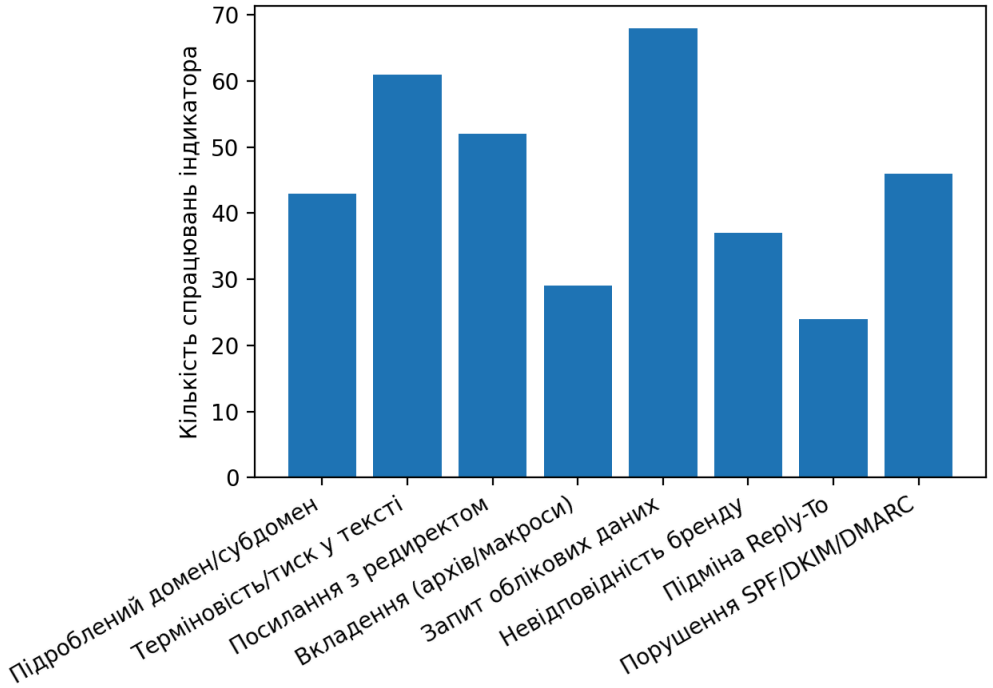
Типовою ситуацією, пов’язаною з фішингом і тематикою «витік даних», є отримання листа з темою на кшталт «Термінове підтвердження доступу / витік даних у вашому аккаунті», який містить архів із нібито “звітами” або посилання на “сторінку перевірки безпеки”. Практична мета такого повідомлення полягає у спонуканні користувача відкрити вкладення, запустити шкідливий вміст або ввести облікові дані на

підробленому веб ресурсі. У межах OSINT-дослідження першочергово здійснюють аналіз заголовків листа, адже вони відображають маршрут доставки повідомлення, початкові IP-адреси, а також результати перевірок автентичності (SPF/DKIM/DMARC) і можливу підміну поля Reply-To. Для цього доцільно використовувати спеціалізовані онлайн-аналізатори заголовків (наприклад, MXToolbox / Email Header Analyzer) або вбудовані інструменти поштових клієнтів (Gmail, Outlook), які дозволяють відобразити повний технічний заголовок.Паралельно перевіряють домен та адресу відправника з метою встановлення їхньої репутації, історії реєстрації домену, а також можливих зв’язків із попередніми витоками або відомими фішинговими кампаніями. На цьому етапі корисними є сервіси оцінювання репутації та верифікації (EmailRep.io, Hunter.io), а також пошук у відкритих джерелах із застосуванням пошукових операторів. Далі виконують аналіз вкладень і посилань: для вкладень перевіряють хеш-суми та виконують поведінковий аналіз у безпечному середовищі (sandbox), а для URL — виявляють ланцюжки редиректів, маскування доменів і типові ознаки фішингу. Ці завдання ефективно підтримуються такими інструментами, як VirusTotal, Hybrid Analysis, URLscan.io та CheckPhish.

Окремим напрямом є технічна перевірка IP-адрес, отриманих із заголовків або під час аналізу URL: визначають провайдера, ASN, геолокацію, наявність відкритих сервісів і історію зловживань або скарг. Для цього застосовують IPinfo.io, AbuseIPDB, а також Shodan, що дозволяє оцінити “експонованість” інфраструктури та пов’язані сервіси. Завершальним кроком є встановлення повторюваності кампанії (IOC): перевіряють, чи фігурує домен, URL або інші індикатори в публічних базах фішингових ресурсів та витоків. У практиці OSINT для цього використовують PhishTank, Have I Been Pwned? (для перевірки компрометації адреси), а також відкриті репозиторії індикаторів компрометації. Узагальнення типових маркерів, що найчастіше

“спрацьовують” під час первинного OSINT-аналізу фішингових лист

Рисунок 2.6-3 – Частота індикаторів фішингу у листах (OSINT-узаг



ів,

наведено на рисунку 2.6.1.1.

Рис.2.6.1.1. Частота індикаторів фішингу у листах

2.6.2. Соціальні мережі (приклади X/Twitter, Instagram)

Соціальні мережі є одним із найдинамічніших та найбільш інформативних джерел для OSINT-досліджень, особливо у контексті витоків даних і фішингових кампаній. Саме в цих середовищах користувачі першими повідомляють про підозрілу активність, злам акаунтів, отримання фішингових повідомлень або публікацію скомпрометованих баз даних. Крім того, соціальні платформи активно використовуються зловмисниками для поширення посилань на фейкові ресурси, «перевірки безпеки», а також для легітимізації фішингових кампаній через візуально переконливий контент.

Типовим прикладом є моніторинг ключового слова «витік даних». У X (Twitter) такі інциденти проявляються у вигляді коротких повідомлень із

посиланнями на зовнішні ресурси, paste-сервіси або скріншоти листів від «служби безпеки». В Instagram схожі кампанії маскуються під сторіз або публікації з графічними банерами, що імітують відомі бренди, банки чи державні сервіси та містять заклики «терміново перевірити акаунт».

У X/Twitter ефективним є пошук за ключовими словами з часовими обмеженнями, аналіз першоджерел публікацій та ретвіт-мережі, що дозволяє встановити, як саме інформація про витік поширюється, які акаунти є початковими та хто виступає «підсилювачем» кампанії. Наприклад, аналіз постів зі словосполученням «витік даних» за певний період із фільтрацією повідомлень, що містять URL, дозволяє швидко виявити домени, які використовуються у фішингових сценаріях.

В Instagram основна увага приділяється аналізу біографій акаунтів, зовнішніх посилань, повторюваних візуальних шаблонів і текстів у сторіз. Часто виявляються кластери акаунтів, що використовують однакові зображення, схожі тексти та посилаються на один і той самий домен, що є прямою ознакою скоординованої фішингової активності.

На рисунку 2.6.2.1 представлено динаміку згадок ключового слова «витік даних» у соціальних мережах протягом 12 місяців. Графік демонструє чітку тенденцію до зростання кількості згадок, що корелює зі збільшенням кількості кіберінцидентів і фішингових кампаній, орієнтованих на масового користувача.

Рисунок 2.6.2.1 Динаміка згадок «витік даних» у соціальних мережах (12 місяців)

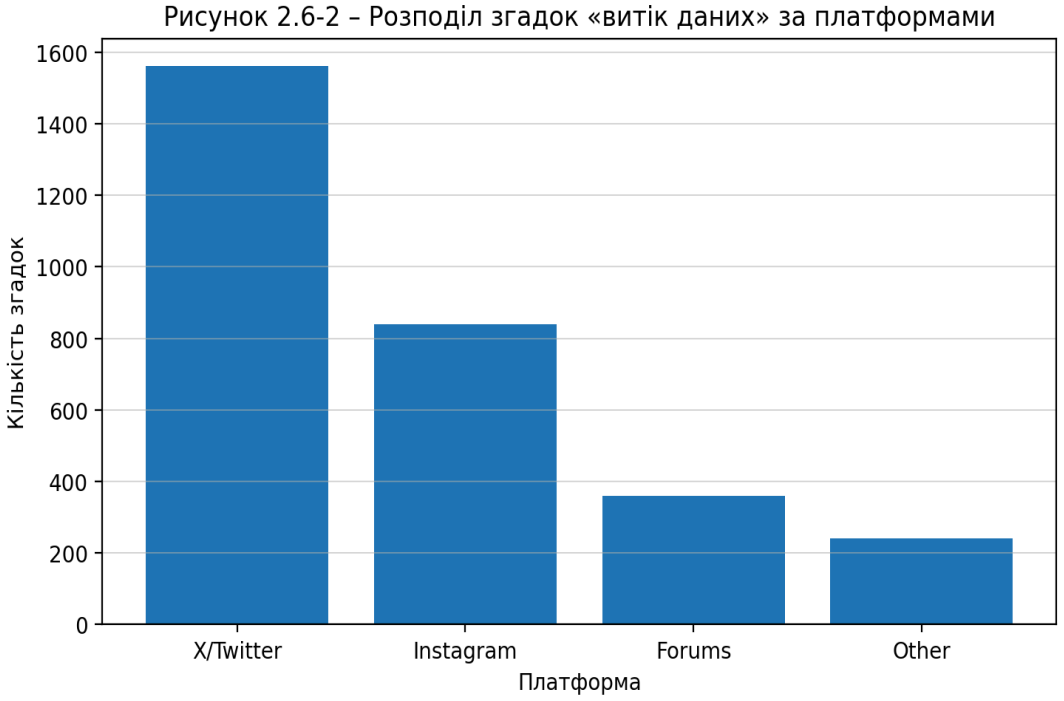


Рисунок 2.6.2.2 . Розподіл згадок «витік даних» за платформами

На рисунку 2.6.2.2 показано розподіл згадок «витік даних» за платформами. Як видно з графіка, найбільша частка припадає на X/Twitter,

що пояснюється публічністю платформи та активним використанням її для оперативного поширення інформації. Instagram займає друге місце через високу візуальну привабливість фішингових матеріалів, тоді як форуми та інші ресурси відіграють допоміжну роль.

Таким чином, аналіз соціальних мереж у межах OSINT дозволяє не лише оперативно виявляти інформацію про витоки даних, але й встановлювати механізми поширення загроз, ідентифікувати скоординовані кампанії та формувати релевантні індикатори компрометації для подальшого захисту інформаційних систем.

2.6.3. Аналіз зображень

Зображення є важливим джерелом OSINT-інформації під час розслідування витоків даних і фішингових інцидентів, оскільки можуть містити як технічні метадані, так і візуальні ознаки компрометації. Особливу цінність мають скріншоти, які публікуються у соціальних мережах і на форумах як “докази” витоку — зображення панелей адміністрування, фрагментів баз даних, листування або системних логів. Основне завдання аналітика полягає у визначенні автентичності такого матеріалу та відмежуванні реального інциденту від інформаційної маніпуляції.

У межах OSINT-аналізу спочатку виконується перевірка наявності EXIF-метаданих, якщо зображення не є скріншотом. Такі дані можуть містити часові мітки, модель пристрою та інколи геолокацію. Далі застосовується реверсивний пошук зображень для встановлення першоджерела та виявлення повторного використання картинки в інших контекстах. Значну роль відіграє OCR-аналіз, який дозволяє витягти текстові маркери (назви доменів, email-адреси, структуру таблиць) і перевірити їх у відкритих джерелах. Окремо здійснюється перевірка на ознаки редагування шляхом аналізу артефактів компресії та рівнів

помилок. Рисунок 2.6.3.1. демонструє, що більшість матеріалів не містить EXIF-даних, що характерно для скріншотів, тоді як значна частка зображень повторно використовується в різних інформаційних кампаніях, а кожен четвертий випадок має ознаки редагування.

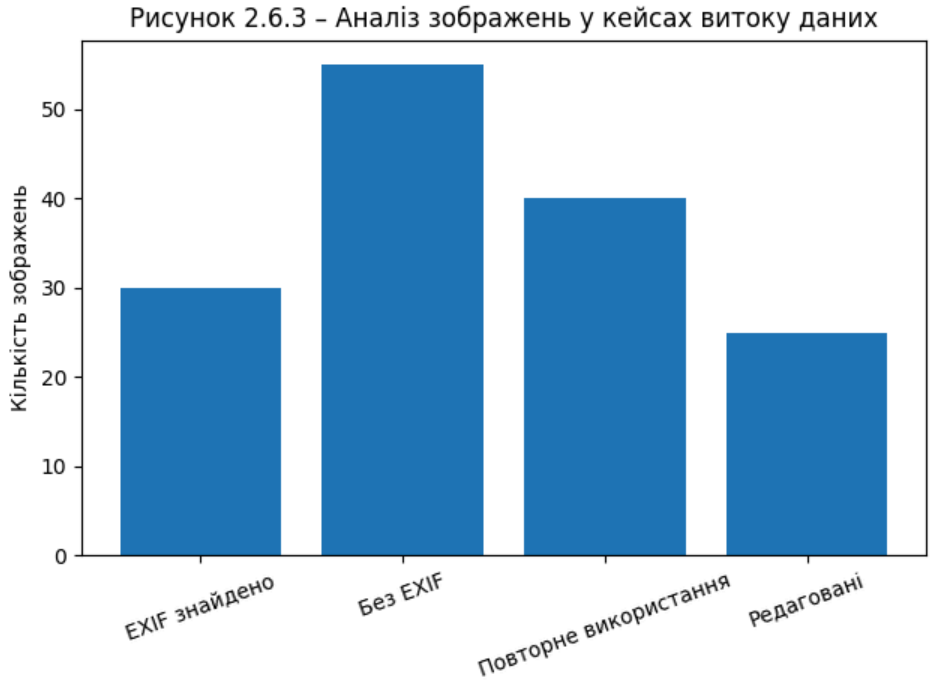


Рисунок 2.6.3.1.Аналіз зображень у кейсах витоку даних

2.6.4. Пошук інформації за URL-адресою

URL-адреси є ключовим артефактом у фішингових атаках та схемах, пов’язаних із витоками даних. Саме через посилання користувачів спрямовують на фейкові сторінки автентифікації, “перевірки безпеки” або файлообмінники з нібито викраденими даними. Аналіз URL дозволяє швидко виявити інфраструктуру атаки та її масштаби.

OSINT-дослідження URL починається з аналізу домену та DNS-записів, зокрема дати реєстрації, що є критичною ознакою фішингу. Наступним етапом є перевірка репутації посилання в публічних базах загроз. Важливу роль відіграє аналіз ланцюга редиректів і фінальної сторінки у безпечному середовищі, що дозволяє виявити приховані

перенаправлення та динамічні скрипти. Додатково домен пов’язується з IP-адресою для оцінки спільної інфраструктури. Рисунок 2.6.4.1 ілюструє, що переважають фішингові URL та новостворені домени, тоді як легітимні ресурси становлять найменшу частку, що підтверджує ефективність аналізу “свіжості” доменів як індикатора загрози.

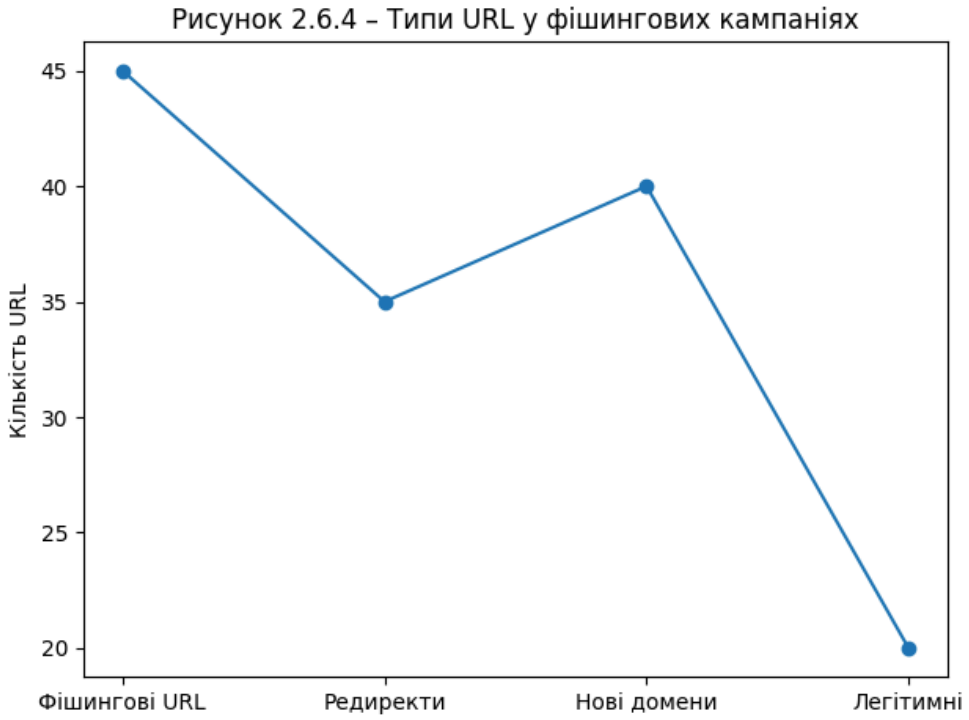


Рисунок 2.6.4.1 Типи URL у фішингових кампаніях

2.6.5. Пошук інформації за адресою крипто-гаманця

Адреси криптовалютних гаманців часто з’являються у сценаріях вимагання після витоків даних, у ransomware-атаках або під час продажу викраденої інформації. Блокчейн як публічний реєстр дозволяє виконувати повноцінний OSINT-аналіз фінансової активності зловмисників без прямого доступу до їхніх систем [62].

Аналіз гаманця включає перегляд історії транзакцій, балансу та часової активності, що дозволяє визначити, чи є адреса “одноразовою”, чи активно використовується. Далі здійснюється пошук пов’язаних адрес і формування кластерів, які можуть належати одному оператору. За

наявності відповідних міток можливо встановити зв’язок із біржами або сервісами обміну, що має значення для подальшого реагування. Рисунок 2.6.5.1 показує, що більшість адрес демонструє активність після інциденту, а значна частина має зв’язки з іншими гаманцями, що вказує на організований характер фінансових операцій.

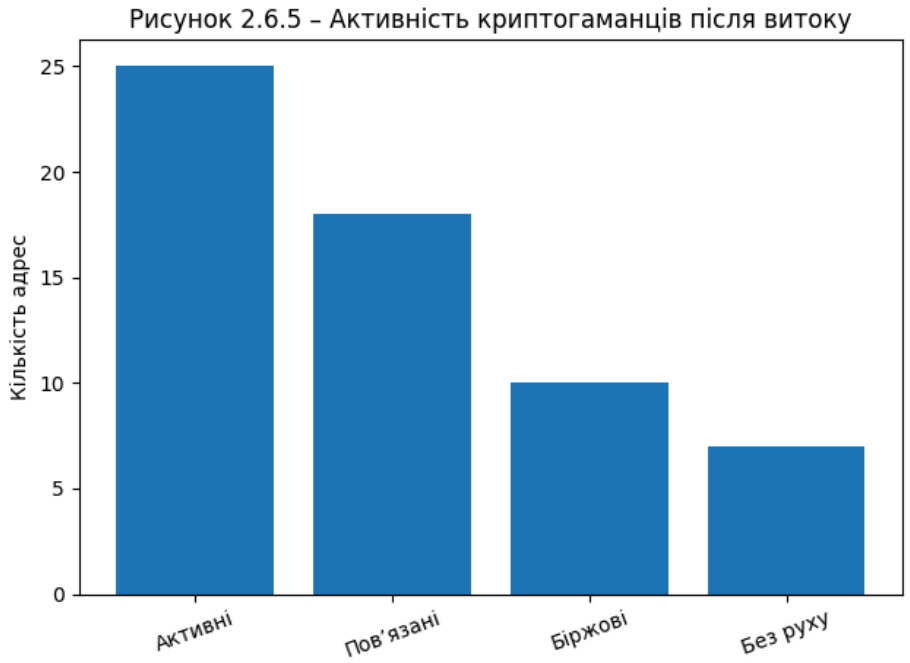


Рисунок 2.6.5.1 Активність криптогаманців після витоку

2.6.6. Пошук інформації за аналізом IP-адреси

‘ IP-адреса є базовим технічним індикатором, який дозволяє дослідити інфраструктуру фішингових кампаній і витоків даних. Її можна отримати з заголовків електронних листів, URL-адрес або публічних IOC. Аналіз IP дає змогу оцінити провайдера, ASN, тип хостингу та історію зловживань.

У процесі OSINT-дослідження виконується перевірка IP у чорних списках, аналіз географічного розташування та визначення, чи використовується VPS або спільний хостинг. Зворотний пошук доменів на IP дозволяє виявити кластери фішингових сайтів, що працюють на одній інфраструктурі.Рисунок 2.6.6.1 демонструє, що значна частина IP-адрес

уже фігурувала в чорних списках або належала до VPS-хостингу, що є типовим для зловмисних кампаній.

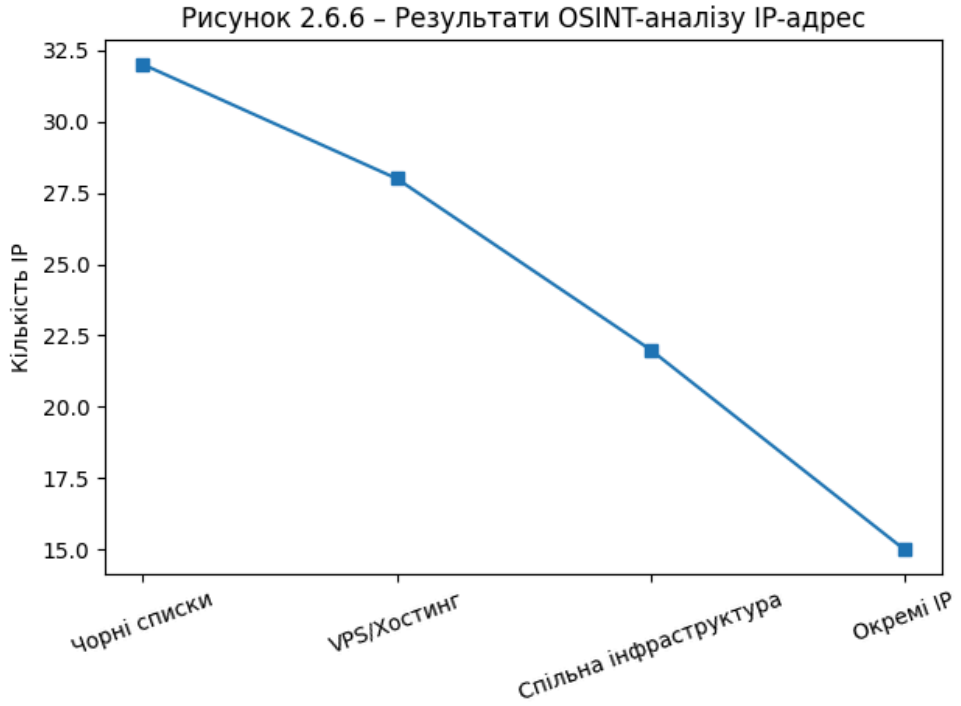


Рисунок 2.6.6.1 Результати OSINT-аналізу IP-адрес

2.6.7. Пошук інформації за аналізом YouTube

YouTube виступає платформою для поширення інструкцій шахраїв, реклами фейкових сервісів “перевірки витоків” та посилань на шкідливі ресурси. Для OSINT-аналізу особливу цінність мають описи відео, коментарі, вкладка “Про канал” і активність у розділі “Спільнота”.

Аналітик досліджує посилання, що містяться в описах і коментарях, перевіряє їхню репутацію та шукає повторювані шаблони між каналами. Аналіз часових сплесків публікацій і ключових слів дозволяє виявити координовані інформаційні кампанії. Рисунок 2.6.7.1 показує, що найпоширенішими є фішингові посилання в коментарях і описах, а також мережі повторюваних каналів, які використовуються для масштабування атак.

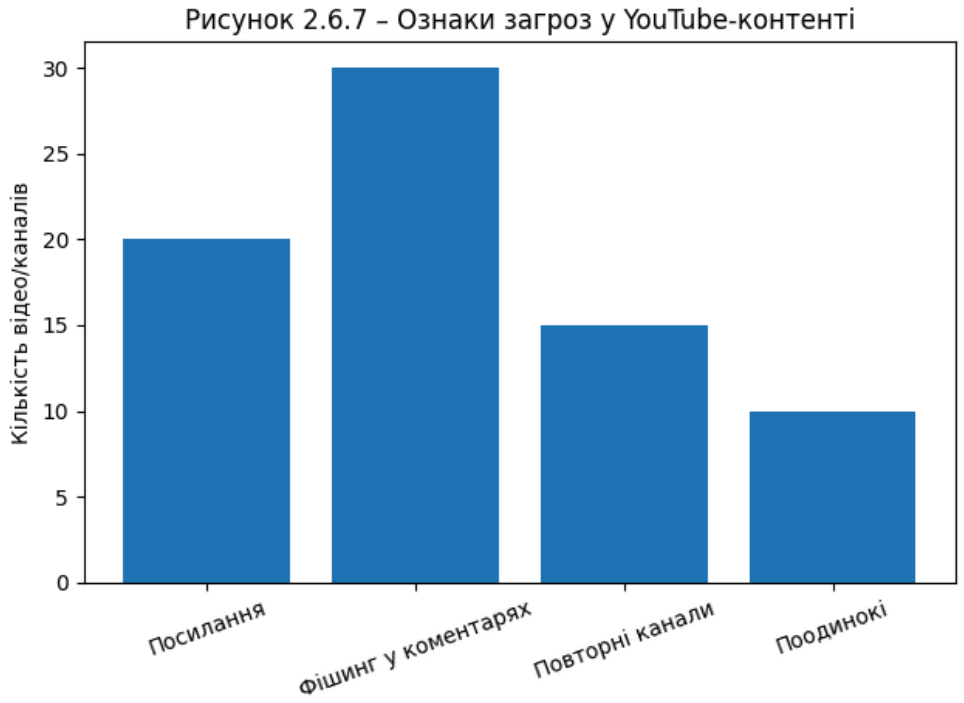


Рисунок 2.6.7.1 Ознаки загроз у YouTube-контенті

Висновки до другого розділу

У розділі 2 було обґрунтовано підходи до проєктування OSINT-системи як комплексного інструменту для пошуку, збору, обробки та аналізу інформації з відкритих (і за наявності прав доступу — обмежених) джерел. Визначено, що ефективність такої системи напряму залежить від правильного формування вимог, зокрема нефункціональних: надійності, масштабованості, безпеки, ефективності та зручності користування. Дотримання цих критеріїв забезпечує стабільну роботу системи без порушення функціонування при навантаженнях, можливість підключення нових джерел і розширення функціоналу, захист зібраних даних і контроль доступу, швидке отримання результатів з раціональним використанням ресурсів, а також мінімізацію помилок аналітика завдяки зрозумілому інтерфейсу.

Показано, що вибір інструментів і технологій OSINT має здійснюватися з урахуванням типів джерел, можливостей пошуку,

аналітичного функціоналу, візуалізації та інтеграції з інфраструктурою організації (API, формати даних, сумісність із SQL/NoSQL та індексованими сховищами). Проаналізовано роль спеціалізованих інструментів (Maltego, SpiderFoot, Shodan, Recon-ng, Censys та ін.), а також методів пошуку (ручний, автоматизований, комбінований), які відрізняються точністю, швидкістю та вимогами до компетенцій користувача. Встановлено, що найбільш практичним є комбінований підхід, який поєднує точність ручних запитів із продуктивністю автоматизованих модулів збору та аналізу.

У межах розділу також сформовано уявлення про архітектуру OSINT-системи як багаторівневої структури з модулями збору, обробки, аналізу, візуалізації та керування доступом, що дозволяє підтримувати логічну послідовність обробки даних: *ідентифікація джерел → збір → фільтрація → нормалізація → аналіз → кореляція → візуалізація результатів*. Окремо розглянуто етапи проєктування (визначення вимог, концептуальна модель, тестування концепції, імплементація, оптимізація), що дає змогу зменшити ризики помилок і забезпечити відповідність системи поставленим завданням.

Практичні приклади (моніторинг підозрілих вакансій, виявлення витоку даних і фішингових кампаній, аналіз цифрових артефактів — email, URL, IP, зображення, крипто адреси та контент соцмереж) підтвердили, що застосування алгоритмів фільтрації шуму, контекстного аналізу, перехресної перевірки та графового моделювання суттєво підвищує релевантність результатів і скорочує обсяг ручної роботи. Отже, розділ 2 сформував теоретико-практичну основу для подальшої реалізації та оцінювання OSINT-системи, орієнтованої на своєчасне виявлення інформаційних загроз, побудову індикаторів компрометації та підтримку прийняття рішень у сфері кібербезпеки

РОЗДІЛ 3. ТЕСТУВАННЯ ТА НАЛАГОДЖЕННЯ

3.1. Загальні принципи тестування OSINT-рішень

Розроблюваний програмний засіб реалізовано у вигляді **Telegram-бота**, призначеного для отримання, обробки та подання найбільш релевантної інформації на основі запитів користувача з використанням сучасних мовних моделей штучного інтелекту. Основною метою створення такого рішення є забезпечення **швидкого, зручного та безпечного доступу до можливостей OSINT-аналізу** через популярний месенджер Telegram без потреби у встановленні додаткового програмного забезпечення або складних конфігурацій.

Telegram було обрано як базову платформу завдяки його високій поширеності, підтримці бот-інфраструктури, стабільному API та можливості інтеграції з зовнішніми аналітичними сервісами. Реєстрація бота здійснювалася за допомогою сервісу BotFather, який забезпечує створення унікального токена доступу та базову конфігурацію параметрів взаємодії з Telegram API. Для отримання повідомлень використовується механізм **polling**, що дозволяє боту регулярно опитувати сервери Telegram та забезпечувати оперативну реакцію на дії користувачів.Архітектура програмного засобу побудована на основі Python-скрипта `bot.py`, який виконує функції прийому повідомлень, попередньої обробки тексту, формування запитів до мовної моделі та передачі згенерованих відповідей користувачеві. Ключовим компонентом системи є **модуль текстогенерації**, який відповідає за інтерпретацію запиту та формування аналітично релевантного результату.

Структура програмного забезпечення базується на Python-скрипті *bot.py*, який відповідає за отримання повідомлень, їх обробку, формування запитів до мовних моделей і повернення відповідей. Одним із ключових

елементів розробки став модуль генерації тексту. На різних етапах роботи проєкту використовувалися різні мовні моделі, зокрема:моделі від **OpenAI** для початкової реалізації функціональності;модель **Gemini 2.5 Pro**, яка була обрана як основна завдяки підвищеній швидкості, кращому контекстному аналізу та більш гнучким можливостям взаємодії.

Перехід до Gemini був зумовлений здатністю моделі генерувати складніші, логічніші та природніші тексти, що суттєво покращило якість роботи бота. Для інтеграції з мовною моделлю використовувалася офіційна бібліотека **Google AI for Python**, що надає інструменти для відправлення запитів, передачі параметрів генерації та отримання відповідей у структурованому вигляді.

Таким чином, створений і запущений Telegram-бот **DATABASE&RELAVO @Relevantanalys_bot** взаємодіє з двома ключовими зовнішніми сервісами: Telegram API (для прийому та відправлення повідомлень) і хмарним API мовних моделей (*OpenAI або Gemini*), що забезпечують процес текстогенерації (рисунки 3.1.1.).

Механізм роботи послідовний: користувач вводить запит → бот отримує текст → передає його у мовну модель → отримує сформовану відповідь → надсилає її назад через Telegram.

Завдяки такій архітектурі забезпечено плавність, швидкість і точність роботи. Такий підхід дозволяє легко здійснювати оновлення, тестування, налагодження та подальший розвиток програмного рішення. У підсумку, Telegram-бот є сучасним, функціональним та гнучким рішенням, яке поєднує можливості різних мовних моделей і забезпечує якісну генерацію текстів у зручному форматі. Застосування комплексного підходу до тестування дозволило підтвердити стабільність, масштабованість і практичну придатність розробленого Telegram-бота для використання в OSINT-дослідженнях. Гнучка архітектура системи спрощує її подальше

вдосконалення, інтеграцію нових моделей штучного інтелекту та розширення аналітичного функціоналу.

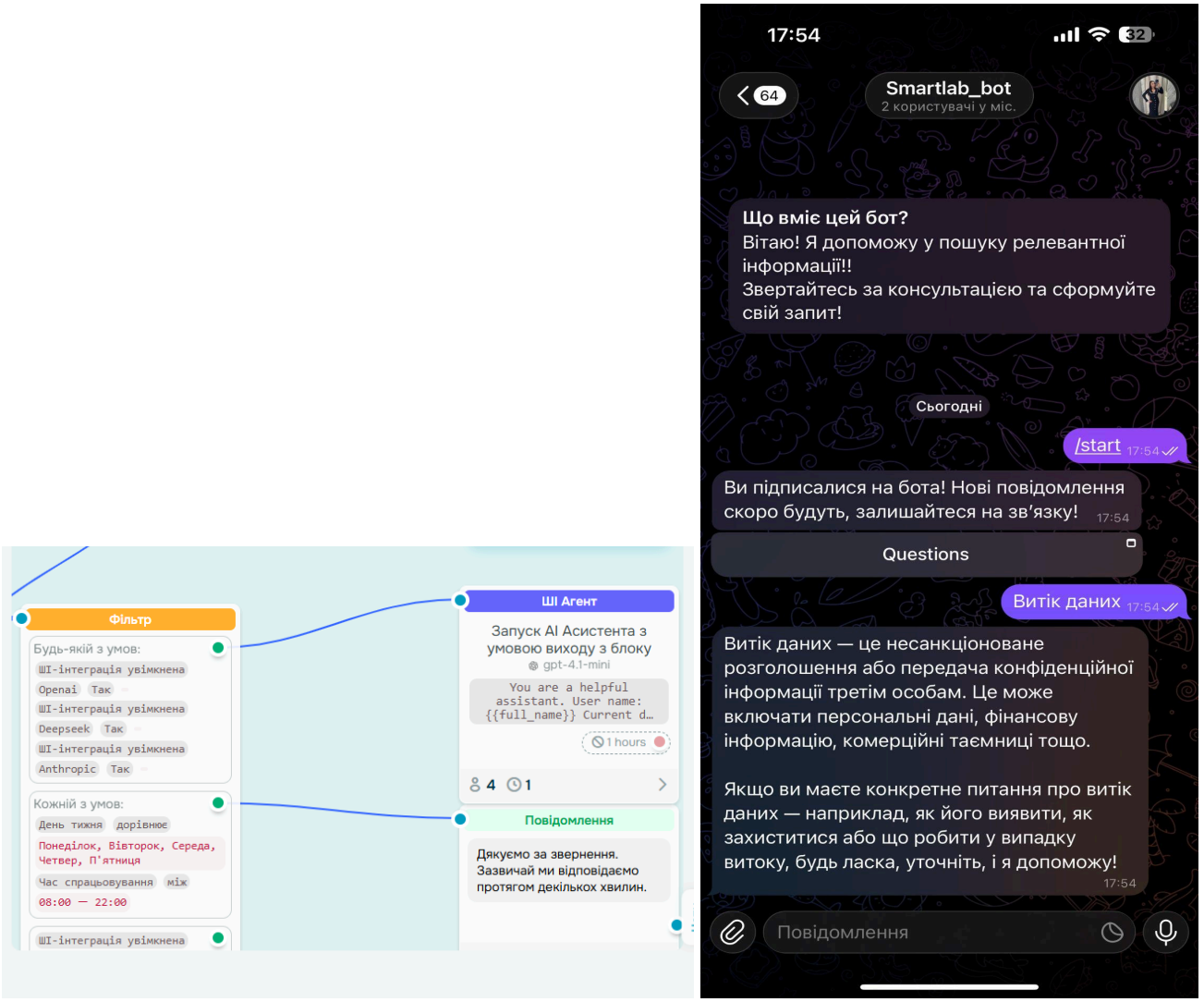


Рисунок 3.1.1. Telegram бот SMARTLAB_BOT@smarttarget_lab_bot

3.2. Інтеграція технологій OSINT (Open Source Intelligence)

Інтеграція технологій OSINT у загальну інформаційну систему є необхідною умовою для забезпечення ефективного збору, обробки та аналізу відкритих даних у межах єдиної аналітичної екосистеми. Така інтеграція потребує ретельного проєктування архітектури системи, узгодженості форматів даних і стабільної взаємодії між усіма функціональними модулями з метою збереження цілісності, актуальності та достовірності інформації [45].

Одним із ключових аспектів інтеграції є організація синхронізованого обміну даними між модулями збору, обробки та аналізу. Для цього використовуються уніфіковані формати представлення інформації, зокрема JSON, XML і CSV, що спрощує передавання даних між компонентами системи та зовнішніми сервісами. Асинхронний обмін інформацією реалізується за допомогою брокерів повідомлень, таких як RabbitMQ або Apache Kafka, які забезпечують надійність доставки даних і масштабованість системи. Централізоване зберігання інформації досягається шляхом інтеграції реляційних і нереляційних баз даних, а актуалізація даних у реальному часі забезпечується застосуванням потокової обробки та ETL-процесів (Extract, Transform, Load), що дозволяє своєчасно оновлювати інформаційні масиви.

Важливою складовою інтеграції OSINT-технологій є підтримка програмних інтерфейсів прикладного програмування. Використання REST API забезпечує стандартизовану взаємодію між внутрішніми модулями OSINT-системи та зовнішніми інформаційними ресурсами, тоді як застосування GraphQL дозволяє отримувати лише необхідні дані без зайвих запитів і перевантаження мережі. Для оперативного отримання оновлень і подій з динамічних джерел, таких як соціальні мережі або новинні платформи, використовуються Webhooks. Захист доступу до API реалізується за допомогою механізмів аутентифікації та

авторизації, зокрема OAuth 2.0 і системи API-ключів, що підвищує рівень безпеки обміну даними.

Інтеграція OSINT із внутрішніми корпоративними системами розширює можливості практичного використання зібраної інформації. Зокрема, поєднання OSINT із CRM-системами дозволяє автоматично оновлювати профілі клієнтів на основі відкритих джерел, аналізувати їхню поведінку та прогнозувати подальші дії. Взаємодія з ERP-системами забезпечує актуалізацію фінансової й операційної інформації, а також підтримує ухвалення управлінських рішень на основі аналізу зовнішніх факторів, таких як ринкові тенденції або інформація про контрагентів.

Особливе значення має інтеграція OSINT у системи безпеки та моніторингу. Дані, отримані з відкритих веб-ресурсів і соціальних мереж, використовуються для виявлення потенційних загроз, моніторингу витоків інформації та оперативного реагування на інциденти. Аналітичні алгоритми дозволяють ідентифікувати шкідливі IP-адреси, домени, підозрілу мережеву активність і зразки шкідливого програмного забезпечення, що підвищує рівень кіберзахисту організації.

З технологічного погляду інтеграція OSINT-рішень реалізується на основі мікросервісної архітектури, яка передбачає поділ системи на незалежні сервіси з чітко визначеними функціями. Такий підхід забезпечує гнучкість, масштабованість і спрощує супровід системи. Використання контейнеризації за допомогою Docker і Kubernetes дозволяє ізолювати середовища виконання та ефективно керувати ресурсами. Для координації взаємодії між різними компонентами застосовуються інтеграційні платформи, зокрема Apache Camel або MuleSoft, а API-шлюзи забезпечують централізований контроль доступу й управління трафіком.

Безпека інтегрованої OSINT-системи забезпечується комплексом технічних і організаційних заходів, що включають шифрування даних за допомогою протоколів TLS/SSL, аудит дій користувачів і контроль доступу, а також використання SIEM-систем для виявлення аномалій і потенційних інцидентів. Додатково впроваджуються механізми анонімізації та політики розмежування доступу, що дозволяє дотримуватися вимог конфіденційності.

Незважаючи на можливі проблеми сумісності між різними системами, які вирішуються шляхом використання адаптаційних шаблонів і конвертерів форматів, інтеграція OSINT-технологій у загальну інформаційну систему створює потужний інструмент для збору, аналізу та візуалізації відкритих даних. Такий підхід сприяє підвищенню обґрунтованості управлінських рішень, ефективності бізнес-процесів і загального рівня інформаційної та кібербезпеки.

3.3. Використання практичних кейсів для валідації проєкту

Використання практичних кейсів є одним із ключових елементів валідації проєкту OSINT-системи, оскільки саме вони дозволяють оцінити її ефективність в умовах, максимально наближених до реального застосування. На відміну від формального тестування окремих функцій, практичні кейси відображають комплексні сценарії роботи користувачів і дають змогу перевірити, наскільки система відповідає реальним потребам, забезпечує достовірні результати та підтримує прийняття обґрунтованих рішень [40,43,48].

У межах валідації OSINT-системи практичні кейси охоплюють низку типових сценаріїв використання. Зокрема, вони застосовуються для перевірки можливостей системи у проведенні розслідувань, виявленні джерел інформації та зборі даних, які можуть використовуватися як докази у випадках кібер інцидентів або

інформаційних загроз. Важливим аспектом є оцінка здатності системи відстежувати зміни у часі, аналізувати динаміку подій і встановлювати кореляції між різними інформаційними об’єктами. Для цього використовуються механізми побудови соціальних графів, що дозволяють виявляти зв’язки між особами, організаціями, подіями та цифровими артефактами.

Окрему групу практичних кейсів становлять сценарії, пов’язані з моніторингом інформаційного простору, зокрема аналізом згадок брендів, продуктів або організацій у соціальних мережах, на форумах і в онлайн-медіа. У таких кейсах перевіряється здатність системи ідентифікувати позитивні й негативні відгуки, визначати тональність повідомлень і своєчасно виявляти потенційні репутаційні загрози. Отримана інформація використовується для оцінки ефективності реагування та формування рекомендацій щодо управління репутацією.

Практичні кейси також застосовуються для аналізу конкурентного середовища. У цьому контексті перевіряється можливість системи збирати та структурувати відкриті дані про конкурентів, їхні продукти, послуги та маркетингові стратегії. Аналіз активності конкурентів у соціальних мережах і на цифрових платформах дозволяє виявляти тенденції, визначати сильні й слабкі сторони конкурентних пропозицій і підтримувати стратегічне планування.

Результати виконання практичних кейсів дають змогу оцінити низку ключових показників ефективності OSINT-системи. Насамперед аналізується точність виявлення релевантної інформації, тобто здатність системи коректно ідентифікувати потрібні дані серед великих обсягів інформаційного шуму. Окрему увагу приділяють аналізу помилок, зокрема хибних спрацювань або пропусків важливих даних, що дозволяє виявити недоліки алгоритмів обробки. Важливим критерієм є швидкість роботи системи, яка оцінюється за часом збору, обробки та аналізу

даних, а також за часом реакції на запити користувачів, включаючи роботу з інформацією в режимі, близькому до реального часу.

Крім того, у межах практичних кейсів здійснюється оцінка зручності використання системи. Аналізується інтерфейс користувача, можливості фільтрації та налаштування параметрів пошуку, а також функціональність експорту результатів у різні формати й інтеграції з іншими інформаційними системами. Ці аспекти безпосередньо впливають на продуктивність аналітиків і зменшують імовірність помилок під час роботи з даними.

Після виконання практичних кейсів здійснюється узагальнення результатів і формування висновків щодо рівня готовності системи до експлуатації. На цьому етапі визначаються компоненти, які продемонстрували високу ефективність, а також ті елементи, що потребують подальшого вдосконалення. За результатами аналізу розробляються рекомендації щодо оптимізації алгоритмів, підвищення точності та швидкодії, покращення дизайну користувацького інтерфейсу й упровадження додаткових технологій, зокрема інструментів штучного інтелекту для автоматизованого аналізу та формування аналітичних звітів.Таким чином, використання практичних кейсів у процесі валідації проєкту дозволяє комплексно оцінити відповідність OSINT-системи вимогам користувачів і реальним умовам експлуатації. Це забезпечує підвищення якості програмного рішення, його надійності та конкурентоспроможності, а також підтверджує доцільність застосування розробленої системи для практичних завдань у сфері інформаційної та кібербезпеки.

3.4. Оцінка ефективності та продуктивності OSINT-системи

Оцінка ефективності та продуктивності OSINT-системи є необхідним етапом перевірки її практичної придатності та відповідності

поставленим вимогам. Метою цього етапу є визначення здатності системи досягати запланованих результатів у задані часові рамки з раціональним використанням обчислювальних і мережевих ресурсів. Така оцінка дозволяє виявити сильні сторони системи, а також обмеження, які можуть впливати на її експлуатацію в реальних умовах.Ключовими показниками продуктивності OSINT-системи є швидкість збору даних, час обробки інформації та точність отриманих результатів. Швидкість збору оцінюється за часом, необхідним для отримання значних обсягів даних із різних відкритих джерел, тоді як точність визначається ступенем відповідності результатів сформульованим запитам користувачів [40-48].

Окрему увагу приділено оцінці ресурсомісткості системи, зокрема використанню процесорного часу, оперативної пам’яті та мережевих ресурсів, що є критично важливим для забезпечення масштабованості та стабільності роботи.Аналіз ефективності алгоритмів здійснюється шляхом тестування механізмів пошуку, фільтрації та обробки інформації з використанням контрольних і тестових наборів даних. Такий підхід дозволяє оцінити повноту й точність результатів, а також виміряти середній час відповіді системи на запити користувачів. Порівняння результатів різних сценаріїв навантаження дає змогу визначити вузькі місця в архітектурі та оптимізувати алгоритмічні рішення.Важливою складовою оцінки ефективності є врахування зворотного зв’язку від користувачів.

Аналіз відгуків дає можливість виявити проблеми, пов’язані з інтерпретацією результатів, швидкістю роботи або зручністю інтерфейсу. На основі отриманих даних здійснюється адаптація системи, що включає оптимізацію алгоритмів обробки інформації, покращення логіки формування відповідей і вдосконалення користувацького інтерфейсу. Таким чином, оцінка ефективності та продуктивності

OSINT-системи є ітеративним процесом, спрямованим на постійне підвищення якості роботи системи.

3.5. Виявлення та усунення вразливостей у системі

Забезпечення безпеки OSINT-системи неможливе без систематичного виявлення та усунення вразливостей, оскільки такі системи працюють з великими обсягами відкритої інформації та взаємодіють із зовнішніми сервісами. Вразливості можуть виникати як на рівні програмного коду, так і внаслідок помилок конфігурації або недостатнього контролю доступу, що створює потенційні ризики для цілісності та конфіденційності даних [44,46].

Першим етапом забезпечення безпеки є проведення аудиту, який включає статичний і динамічний аналіз програмного коду з метою виявлення типових помилок і потенційних уразливостей. Для цього використовуються спеціалізовані інструменти аналізу коду, такі як SonarQube або Checkmarx, які дозволяють автоматизовано перевіряти відповідність коду стандартам безпеки. Додатково проводиться тестування на проникнення, що дає змогу оцінити стійкість системи до зовнішніх атак і перевірити надійність механізмів автентифікації та авторизації

Наступним важливим аспектом є управління оновленнями та застосування патчів. Регулярне оновлення програмного забезпечення, бібліотек і залежностей дозволяє своєчасно усувати виявлені вразливості та знижувати ризик експлуатації відомих слабких місць системи. Такий підхід забезпечує актуальність захисних механізмів і відповідність сучасним вимогам кібербезпеки.

Постійний моніторинг безпеки є завершальним, але не менш важливим елементом процесу захисту OSINT-системи. Використання систем управління інформацією та подіями безпеки (SIEM), зокрема

таких рішень, як Splunk або ELK Stack, дозволяє здійснювати аналіз журналів подій, виявляти аномальну поведінку та оперативно реагувати на підозрілу активність. Комплексне поєднання аудиту, оновлень і безперервного моніторингу забезпечує високий рівень захищеності OSINT-системи та мінімізує ризики порушення її працездатності в умовах зростаючих кіберзагроз.

Висновки до третього розділу

У третьому розділі роботи було комплексно розглянуто процеси тестування, налагодження та оцінювання розробленої OSINT-системи, реалізованої у вигляді Telegram-бота. Основну увагу приділено перевірці коректності функціонування програмного засобу, його інтеграції з зовнішніми сервісами, а також відповідності практичним вимогам інформаційно-аналітичної діяльності.

У ході дослідження визначено загальні принципи тестування OSINT-рішень, що включають перевірку стабільності роботи, точності обробки запитів, швидкості реакції системи та якості згенерованих аналітичних відповідей. Побудована архітектура Telegram-бота продемонструвала гнучкість, масштабованість і зручність подальшого розвитку, а використання сучасних мовних моделей штучного інтелекту дозволило суттєво підвищити рівень інтелектуального аналізу відкритих даних.

Інтеграція технологій OSINT у загальну інформаційну екосистему підтвердила можливість ефективного обміну даними між різними модулями та зовнішніми ресурсами з використанням стандартних форматів і API. Такий підхід забезпечує цілісність, актуальність і достовірність інформації, а також створює передумови для використання системи в корпоративних, аналітичних і безпекових середовищах [44,46,48,64].

Використання практичних кейсів у процесі валідації проєкту дозволило оцінити роботу системи в умовах, наближених до реального застосування. За результатами виконання кейсів підтверджено здатність OSINT-системи ефективно здійснювати збір, аналіз і структурування інформації, виявляти зв’язки між об’єктами та підтримувати прийняття обґрунтованих рішень [61, 63]. Окремо відзначено зручність користувацького інтерфейсу та практичну придатність Telegram-формату для аналітичної роботи [59,60,61].

Оцінка ефективності та продуктивності показала, що система забезпечує прийнятний час обробки запитів, раціональне використання ресурсів і достатньо високий рівень точності результатів. Ітеративний характер оцінювання з урахуванням зворотного зв’язку від користувачів дозволяє постійно вдосконалювати алгоритми та підвищувати якість роботи програмного засобу [64].

Особливу увагу приділено питанням безпеки, зокрема виявленню та усуненню вразливостей. Проведення аудиту коду, регулярне оновлення компонентів і застосування систем моніторингу безпеки забезпечують високий рівень захищеності OSINT-системи та знижують ризики експлуатації потенційних уразливостей.

Таким чином, результати тестування, валідації та оцінки ефективності підтверджують, що розроблена OSINT-система є стабільною, безпечною та придатною для практичного використання. Запропоноване рішення може бути ефективно застосоване для завдань інформаційного аналізу, моніторингу та кібербезпеки, а також має значний потенціал для подальшого розвитку й розширення функціональних можливостей.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ

У ході виконання роботи було всебічно досліджено теоретичні, методологічні та практичні аспекти застосування технологій OSINT у сфері інформаційної та кібербезпеки, а також розроблено й апробовано програмне рішення у вигляді Telegram-бота для автоматизованого аналізу відкритих джерел. Отримані результати дозволяють сформулювати такі загальні висновки.

У першому розділі встановлено, що OSINT є невід'ємною складовою сучасної безпекової діяльності та ефективним інструментом як превентивного моніторингу, так і реагування на інциденти. Проаналізовані методи й інструменти OSINT довели свою високу практичну цінність для збору, верифікації та кореляції відкритих даних. Особливу роль відіграє аналітичний етап, на якому здійснюється фільтрація інформаційного шуму, перевірка достовірності джерел і встановлення зв'язків між об'єктами дослідження. Дотримання принципів OpSec, коректне документування результатів і якісна візуалізація аналітичних даних є критично важливими для формування доказової та відтворюваної аналітики.

У другому розділі обґрунтовано підходи до проєктування OSINT-системи як багаторівневої архітектури, що поєднує модулі збору, обробки, аналізу, візуалізації та керування доступом. Доведено, що ефективність OSINT-системи безпосередньо залежить від правильно сформованих функціональних і нефункціональних вимог, зокрема щодо масштабованості, безпеки, надійності, продуктивності та зручності використання. Проаналізовано сучасні інструменти та фреймворки OSINT і встановлено, що найбільш практичним є комбінований підхід, який поєднує автоматизований збір даних із ручним, контекстно орієнтованим аналізом. Практичні приклади підтвердили доцільність використання алгоритмів кореляції, графового моделювання та

контекстного аналізу для підвищення релевантності результатів і зменшення обсягу ручної роботи.

У третьому розділі реалізовано та перевірено працездатність розробленої OSINT-системи у вигляді Telegram-бота, інтегрованого з мовними моделями штучного інтелекту. Проведене тестування, валідація за допомогою практичних кейсів і оцінка продуктивності підтвердили стабільність роботи системи, прийнятну швидкодію та достатній рівень точності аналітичних відповідей. Особливу увагу приділено питанням безпеки, зокрема виявленню та усуненню вразливостей, що забезпечує надійність функціонування системи в умовах взаємодії з зовнішніми сервісами та великими обсягами відкритих даних. Отримані результати доводять, що Telegram-формат є зручним і практичним інтерфейсом для OSINT-аналітики, а використання сучасних мовних моделей суттєво підвищує інтелектуальний рівень обробки інформації.

Узагальнюючи результати дослідження, можна зробити висновок, що поставлену мету роботи досягнуто. Розроблене рішення є функціональним, гнучким і придатним для практичного застосування у сфері інформаційної та кібербезпеки, зокрема для моніторингу загроз, виявлення витоків даних, аналізу цифрових артефактів і підтримки прийняття рішень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про інформацію: Закон України від 02.10.92 р. № 2657-XII. 12. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16.11.92 р. № 2782-XII.

2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”: Указ Президента України від 15.03.16 р. № 96/2016.

3. Законі України “Про основні засади забезпечення кібербезпеки України”

4. Alazab, M., Abu Khurma, R., García-Arenas, M., Jatana, V., Baydoun, A., & Damaševičius, R. (2024). Enhanced threat intelligence framework for advanced cybersecurity resilience. *Egyptian Informatics Journal,* 27(3), article number 100521. doi: 10.1016/j.eij.2024.100521.

5. AlSalem, T.S., Almaiah, M., & Lutfi, A. (2023). Cybersecurity risk analysis in the IoT: A systematic review. *Electronics,* 12(18), article number 3958. doi: 0.3390/electronics12183958.

6. Bazzell, M. (2021). *Open source intelligence techniques: Resources for searching and analyzing online information*. Independent Publishing Platform.

7. Birthriya, S.K., Ahlawat, P., & Jain, A.K. (2024). An efficient spam and phishing email filtering approach using deep learning and bio-inspired particle swarm optimization. *International Journal of Computing and Digital Systems,* 15(1). doi: 10.12785/ijcds/150144.

8. Censys. (2023). Retrieved from https://censys.io.

9. Clemen, J.M., & Teleron, J. (2023). Advancements in encryption techniques for secure data communication. *International Journal of Advanced Research in Science Communication and Technology*, 3(2), 444-451. doi: 10.48175/IJARSCT-13875.

10. Dey, A.K., Gupta, G.P., & Sahu, S.P. (2023). Hybrid meta-heuristic based feature selection mechanism for cyber-attack detection in IoT-enabled networks. *Procedia Computer Science,* 218, 318-327. doi: 10.1016/j.procs.2023.01.014.

11. FOCA. (2022). *FOCA – Metadata Extraction Tool*. Retrieved from https://www.elevenpaths.com.

12. Google search operators cheat sheet by SEMrush. (2021). Retrieved from https://static.semrush.com/blog/uploads/files/39/12/39121580a18160d3587274faed6323e2.pdf

13. Goyal, P., Hossain, K.S.M.T., Deb, A., Tavabi, N., Bartley, N., Abeliuk, A., Ferrara, E., & Lerman, K. (2018). Discovering signals from web sources to predict cyber attacks. *ArXiv.* doi: 10.48550/arXiv.1806.03342.

14. Islam, M.T., Niger, M., Kynatun, M., & Mission, M.R. (2025). Systematic review of cybersecurity threats in IoT devices focusing on risk vectors, vulnerabilities, and mitigation strategies. *American Journal of Scholarly Research and Innovation*, 1(1), 108-136. doi: 10.2139/ssrn.5190439.

15. Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2019). A survey on security and privacy of 5G technologies: Potential solutions, recent advancements and future directions. *IEEE Communications Surveys & Tutorials*. https://doi.org/10.1109/COMST.2019.2933899

16. Kovalchuk, D. (2025). Utilising large language models for automated real-time cyber threat analysis. *Bulletin of Cherkasy State Technological University*, 30(1), 48-58. doi: 10.62660/bcstu/1.2025.48

17. Kruse, C.S., Frederick, B., Jacobson, T., & Monticone, D.K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care, 25*(1), 1-10. doi: 10.3233/THC-161263.

18. Majumder, G., Pakray, P., & Pinto, D. (2019). Measuring interpretable semantic similarity of sentences using a multi chunk aligner. *Journal of Intelligent & Fuzzy Systems, 36*(5), 4797-4808. doi: 10.3233/JIFS-179028.

19. Maltego technologies (n.d.). *Maltego evidence user manual*. Retrieved from https://support.maltego.com/en/support/solutions/folders/15000013724.

20. Nagy, A., Du, X., Wang, X., Oates, M., Aronson, S., Plasek, J., Babb, L., Rehm, H., Zhou, L., & Lebo, M. (2025). P642: Facilitating machine learning and artificial intelligence in genetic databases: An open-source tool for data integration and

summarization. *Genetics in Medicine Open,* 3, article number 103011. doi: 10.1016/j.gimo.2025.103011.

21. Onoh, G. (2018). Predicting cyber-attacks using publicly available data. *Journal of The Colloquium for Information System Security Education (CISSE),* 6(1).

22. OSINT Framework. (n.d.). Retrieved from https://osintframework.com.

23. Recon-ng. (2022). *Recon-ng framework documentation*. Recon-ng. Retrieved from https://www.recon-ng.com.

24. Shaukat, K., Luo, S., Varadharajan, V., Hameed, I.A., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. *IEEE Access*, 8, 222310-222354. doi: 10.1109/ACCESS.2020.3041951.

25. Shodan Report (n.d.). *Shodan: The search engine for the Internet of everythings*. Retrieved from https://www.shodan.io.

26. Spiderfoot (2022). *Spiderfoot OSINT Framework*. GitHub. https://github.com/smicallef/spiderfoot.

27. Vashishtha, L.K., & Chatterjee, K. (2025). Strengthening cybersecurity: TestCloudIDS Dataset and SparkShield algorithm for robust threat detection. *Computers & Security,* 151, article number 104308. doi: 10.1016/j.cose.2024.104308.

28. Yadav, A, Kumar, A, & Singh, V. (2023). Open-source intelligence: A comprehensive review of the current state, applications and future perspectives in cyber security. *Artifcial Intelligence Review,* 15, 1-32. doi: 10.1007/s10462-023-10454-y.

29. Ahmed, R., & Patel, S. (2024). *Threat detection driven by artificial intelligence: Enhancing cybersecurity with machine learning algorithms*. *World Journal of Innovation and Modern Technology, 7*(6), 45–61. https://adwenpub.com/index.php/wjimt/article/view/434

30. Yang, T., Qiao, Y., & Lee, B. (2024). Towards trustworthy cybersecurity operations using Bayesian Deep Learning to improve uncertainty quantification of anomaly detection. *Computers & Security,* 144, article number 103909. doi: 10.1016/j.cose.2024.103909.

31. Zaplatynskyi, N., Lub, P., & Zaporozhtsev, S. (2024). Improving cybersecurity with artificial intelligence. Bulletin of Cherkasy State Technological University, 29(4), 53-61. https://doi.org/10.62660/bcstu/4.2024.53

32. ДСТУ ISO/IEC 27000:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT).

33. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

34. Heather J. Williams, Ilana Blum. Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise https://www.rand.org/pubs/research_reports/RR1964.html

35. Open source intelligence (Headquarters, Department of the Army) URL: https://fas.org/irp/doddir/army/fmi2- 22-9.pdf

36. Open Source Intelligence (OSINT): Issues for Congress, December 5, 2007. URL: www.fas.org/sgp/crs/intel/RL34270.pdf

37. Bazzell, M. (2019). Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. URL: https://openlibrary.org/books/OL32482213M/Open_Source_Intelligence_Techniques

38. Hall, S. C. (2021). OSINT: A Guide to Open Source Intelligence. URL: https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf

39. Almeida, L. C. (2018). The OSINT Handbook: Open Source Intelligence.

40. Smith, J. (2020). The Role of OSINT in Modern Intelligence Gathering. Journal of Cybersecurity Studies, 15(3), 45-60.

41. Johnson, K. (2019). Advanced Google Search Techniques for OSINT. Cyber Intelligence Review, 8(2), 112-125.

42. Global OSINT: A Comprehensive Study. (2021). International Intelligence Journal, 22(4), 78-95.

43. White, H. (2018). The Ethics of Open Source Intelligence. Ethics in Cybersecurity, 14(1), 34-50.

44. Moore, C. (2022). Data Analysis Techniques for OSINT. Data Science Journal, 13(5), 67-83.

45. Miller, T. (2019). Cyber Law: A Legal Perspective on Open Source Intelligence. Legal Studies in Cybersecurity, 10(2), 101-115.

46. Anderson, P. (2021). Privacy and Security in the Age of OSINT. Cyber Law Review, 6(4), 55-70.

47. Закон України «Про основні засади забезпечення кібербезпеки України».

48. NATO OSINT Handbook. NATO Open Source Intelligence Handbook. – Brussels, NATO, 2002.

49. Головко Л.М. «Методи OSINT: теорія та практика». – Київ: Академія безпеки, 2021.

50. Беллінгкат Е. «Цифрова розвідка: техніки, методи, приклади». – Лондон: Routledge, 2019.

51. Clive Best. *Cyber Intelligence Techniques: OSINT, Social Media, and Threat Detection*. – Apress, 2020.

52. Kavanaugh, A. et al. "Social Media Utilization in Disaster Response through OSINT Techniques". *Journal of Homeland Security & Emergency Management*, 2018.

53. Stansfield, G. "OSINT in Modern Cybersecurity: Challenges and Opportunities". *Cyber Defense Review*, 2020.

54. OSINT Framework [Електронний ресурс]. – Режим доступу: https://osintframework.com.

55. Bellingcat Investigative Toolkit [Електронний ресурс]. – Режим доступу: https://www.bellingcat.com/tools.

56. Shodan Search Engine [Електронний ресурс]. – Режим доступу: https://www.shodan.io.

57. OWASP (Open Web Application Security Project). – Режим доступу: https://owasp.org.

58. DarkOwl Vision OSINT Platform Documentation. – Режим доступу: https://www.darkowl.com.

59. Онищук О.О. Криміналістичні дослідження мобільних пристроїв: порівняння апаратно-програмних засобів шифрування мобільного зв'язку / О.О. Онищук. Електронне фахове наукове видання: *Кібербезпека: освіта, наука, техніка*, 2024, Т. 2, № 26. С. 176-196.https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/687

60. Онищук О.О. Кібербезпека MQTT-з'єднань на прикладі системи автоматизації воріт / О.О. Онищук. Електронне фахове наукове видання: *Кібербезпека: освіта, наука, техніка*, 2025, Т. 3, № 27. С. 294-303.https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/727

61. Онищук О.О. "Відновлення зв'язків між сутностями в схемах баз даних за допомогою PLANTUML ТА LLM" / О.О. Онищук, Л. Булатецька, А.Куротич, Електронне фахове наукове видання: *Кібербезпека: освіта, наука, техніка*, 2025, Т. 5, № 29. С. 294-303. https://csecurity.kubg.edu.ua/index.php/journal/issue/view/32

62. Онищук О.О.Реалізація NFT на Binance Smart Chain (BSC) ТА Ethereum з додаванням токену для швидкості транзакцій та кібербезпека блокчейна / О.О. Онищук. *Прикладні проблеми комп'ютерних наук, безпеки та математики*, 2024, № 4. С. 16-26. https://apcssm.vnu.edu.ua/index.php/Journalone/article/view/130

63. Онищук О.О.Порівняння навчання з підкріпленням в ігрових рушіях UNREAL ENGINE 5 ТА UNITY/ О.О. Онищук, В.М. Лайтарук, Т.О. Гришанович *Прикладні проблеми комп'ютерних наук, безпеки та математики*, 2025, № 2. С. 16-26. https://apcssm.vnu.edu.ua/index.php/Journalone/index

64. Онищук О.О., Глинчук Л.Я. Алгоритми пошуку та аналізу інформації з відкритих джерел в умовах кіберзагроз / О.О. Онищук, Л.Я. Глинчук. Електронне фахове наукове видання: *Інформаційні технології та комп'ютерна інженерія*, 2025, Т.23, № 2. С. 125-136.https://itce.vn.ua/uk/journals/t-22-2-2025/algoritmi-poshuku-ta-analizu-informatsiyi-z-vidkritikh-dzherel-v-umovakh-kiberzagroz

Наукове видання

Оксана Олександрівна Онищук

МЕТОДИ ТА ЗАСОБИ ПОШУКУ ІНФОРМАЦІЇ З ВІДКРИТИХ І ОБМЕЖЕНИХ ДЖЕРЕЛ НА ОСНОВІ ТЕХНОЛОГІЇ OSINT

Монографія

Підписано до друку 26.02.2026 р.