УДК 004.056.53:004.9:338.28 DOI: 10.31673/2786-8362.2025.028204

Вишнівський В.В., д.т.н.; **Іщеряков С.М.,** к.т.н.;
Березовська Ю.В., PhD; **Термко М.О.**

АНАЛІЗ СУЧАСНИХ ПІДХОДІВ КОМП'ЮТЕРНОЇ КОНКУРЕНТНОЇ РОЗВІДКИ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ВІДКРИТИХ ДЖЕРЕЛ

Vyshnivskyi V.V., Ishcheryakov S.M., Berezovska Yu.V., Termko M.O. Analysis of modern approaches to computer competitive intelligence using open source technologies. The article analyzes modern approaches to conducting computer-based competitive intelligence using OSINT (Open Source Intelligence) technologies. The relevance of this topic is determined by the rapid growth of the volume of open data on the Internet and the need for its effective use to enhance the competitiveness of organizations. The purpose of the study is to generalize the methods and tools of computer competitive intelligence based on OSINT technologies, and to determine their capabilities and limitations. Within the study, various approaches and tools used for the collection and analysis of information about the competitive environment from open sources are examined. In particular, methods for monitoring web resources, social networks, blogs, online forums, and open databases are analyzed, which allow the automated search for relevant data on competitors' activities. Special attention is paid to the use of modern software and online services for OSINT, as well as the potential of machine learning technologies and big data processing to increase the efficiency of competitive intelligence. It was found that the use of OSINT ensures broad coverage of information sources and timely acquisition of relevant data. At the same time, effective use of OSINT requires a structured approach to filtering results and verifying the reliability of collected information. The results of the research enable the identification of the advantages and disadvantages of each of the current OSINT-based approaches and tools for competitive intelligence. The practical significance of the obtained results lies in the possibility of using the formulated recommendations to improve competitive intelligence processes and information-analytical activities. The application of modern OSINT approaches will contribute to more informed managerial decision-making and strengthen the competitive positions of organizations in the market.

Keywords: open information sources; web monitoring; social media analytics; data collection tools; machine learning; big data; competitive advantage; decision support

Вишнівський В.В., Іщеряков С.М., Березовська Ю.В., Термко М.О. Аналіз сучасних підходів комп'ютерної конкурентної розвідки із використанням технологій відкритих джерел. У статті проведено аналіз сучасних підходів до здійснення комп'ютерної конкурентної розвідки із застосуванням технологій відкритих джерел, OSINT (розвідки з відкритих джерел). Актуальність теми обумовлена стрімким зростанням обсягу відкритих даних у мережі Інтернет та необхідністю ефективного використання цієї інформації для підвищення конкурентоспроможності організацій. Метою дослідження є узагальнення методів і засобів комп'ютерної конкурентної розвідки, що базуються на технологіях OSINT, а також визначення їх можливостей та обмежень У рамках дослідження розглянуто різноманітні підходи й інструменти, які використовуються для збору та аналітичної обробки інформації про конкурентне середовище з відкритих джерел. Зокрема, проаналізовано методи моніторингу веб-ресурсів, соціальних мереж, блогів, онлайн-форумів та відкритих баз даних, що дозволяють автоматизувати пошук релевантних даних про діяльність конкурентів. Особливу увагу приділено застосуванню сучасних програмних засобів та онлайн-сервісів для OSINT, а також можливостям технологій машинного навчання та обробки великих даних у підвищенні ефективності конкурентної розвідки. Виявлено, що використання OSINT забезпечує широку інформаційну охопленість джерел інформації та оперативність отримання актуальних даних. Водночас застосування OSINT потребує структурованого підходу до фільтрації результатів і перевірки достовірності зібраних даних. Результати дослідження дозволяють визначити переваги і недоліки кожного з сучасних підходів та інструментів OSINT для конкурентної розвідки. Практична значущість отриманих результатів полягає у можливості використання сформульованих рекомендацій для вдосконалення процесів бізнес-розвідки та інформаційно-аналітичної діяльності. Застосування сучасних OSINT-підходів сприятиме більш обґрунтованому прийняттю управлінських рішень і зміцненню конкурентних позицій організацій на ринку.

Ключові слова: відкриті інформаційні ресурси; моніторинг веб-ресурсів; аналіз соціальних мереж; інструменти збору даних; машинне навчання; великі дані; конкурентоспроможність; підтримка прийняття рішень

Вступ

Постановка завдання. В даний період часу, можемо спостерігати надзвичайне зростання промислової діяльності, збільшення інфраструктури, доповнення вже існуючих бізнес рішень

© Вишнівський В.В., Іщеряков С.М., Березовська Ю.В., Термко М.О. 2025

та створення нових. Головною складовою виступає масова комп'ютерізація процесів. Оцифровування або диджиталізація навколишнього проходить шаленими темпами. Потік інформації котрий потрапляє у відкритий доступ в глобальну мережу Інтернет до звичайних користувачів, унеможливлює зворотній процес. Це створює дефрагментоване зображення інформації, зібравши всі потрібні сегменти, є можливість побачити стратегічну складову. Також можна охарактеризувати цей процес, як Open Source Intelligence (OSINT), розвідка на основі відкритих джерел. Ця технологія взяла свій початок в професійному застосуванні в сорок першому році двадцятого століття, до появи сучасного Інтернету. Вона є досить ефективною, але так і не систематизувалась, не сформувалась як алгоритм певних дій у актуалізації зацікавленості, з урахуванням сучасних технологій, за для потенційного розвитку, та збільшення конкурентно спроможності. Таким чином виникає нагальна потреба у аналізі поточних досліджень, структурізації інформації, побудови алгоритмів, методів формування самого об'єкту інформації.

Аналіз останніх досліджень. У сучасних реаліях питання комп'ютерної конкурентної розвідки має усі передумови для активного наукового розвитку та прикладного впровадження. Особливої актуальності дана тематика набула з початком повномасштабної війни в Україні, що суттєво посилило потребу в ефективному зборі, аналізі та використанні інформації з відкритих джерел як у бізнесі, так і в сферах національної безпеки та оборони. Це породило купу ентузіастів, людей котрі в цьому зацікавлені, сформувало групи дослідників, мисливців на інформацію.

Втім, на жаль, не всі представники цієї спільноти дотримуються системного або наукового підходу. Значна частина OSINT-ентузіастів використовує лише базові алгоритми пошуку інформації (Google dorking, перевірка доменів, соціальний граф), зосереджуючись на поверхневих даних без глибокої верифікації, моделювання чи побудови аналітичної логіки. Часто ігнорується потенціал автоматизованих систем аналізу таких як семантичні мережі, ML-моделі класифікації ризиків, багаторівневий моніторинг інформаційних потоків.

Варто зазначити, що ще до початку повномасштабного вторгнення в Україні вже існувала сформована спільнота фахівців, які займалися OSINT-аналізом у різних сферах від журналістики й маркетингу до безпеки й криміналістики. Серед них були як окремі аналітики, так і інституційні групи, що проводили моніторинг відкритих джерел, розробляли методики збирання та інтерпретації інформації. Одним із перших популяризаторів OSINT в Україні є Золотухін Дмитро Юрійович, який демонстрував підходи до відкритої розвідки та заснував освітній проєкт «OSINT Academy» [1], також лекційні матеріали є доступні на платформі youtube[2]. Дмитро Юрійович є керівником громадської організації «Інститут постінформаційного суспільства»[3]. Він активно демонструє підходи до відкритої розвідки, проводить навчальні курси й тренінги для журналістів, фахівців з безпеки та громадських активістів[4].

Разом з тим, позитивним є те, що в Україні існує й активно розвивається коло справжніх науковців, які працюють у напрямі формалізації та автоматизації OSINT. До таких можна віднести групу дослідників під керівництвом Дмитра Володимировича Ланде, яка розробляє архітектури інформаційного аналізу, методи виявлення інформаційних операцій та моделі роботи з великими даними. В їхніх працях OSINT розглядається як складова частина комп'ютерної конкурентної розвідки, що може бути інтегрована у бізнес-процеси, наукові обчислення, оборонні системи.

Таким чином, сьогодні в Україні спів існують два вектори розвитку OSINT. Масовий, оперативно-ентузіастський, що відіграє важливу роль у мобілізації інформаційного суспільства, та глибокий науково-технологічний, який формує підґрунтя для побудови інтелектуальних аналітичних систем майбутнього.

Науковці цієї групи розробили архітектури інформаційного аналізу, методи автоматизованого виявлення інформаційних операцій, а також кластерні моделі обробки тематичних потоків великих обсягів даних [5; 6]. Їхні розробки використовують такі інструменти, як сегментація інформаційного простору, семантичні графи, візуалізація

інформаційних кампаній, що може бути адаптовано до бізнес-розвідки, медіа-моніторингу або оцінки репутаційних ризиків.

Особисто Д. В. Ланде зробив вагомий внесок у формалізацію термінології OSINT, розробив методологію автоматичного виявлення інформаційних операцій [5], а також опублікував та публікує ключові наукові праці, у яких демонструє ефективність застосування автоматизованих підходів до виявлення інформаційних загроз у відкритих джерелах [6; 7]. Його співавторство у монографії «Комп'ютерна конкурентна розвідка» (2021) стало першою в Україні комплексною спробою інтеграції OSINT, інформаційної безпеки, текстового аналізу та big data для підтримки прийняття рішень [8].

У цих розробках OSINT розглядається не лише як інструмент збору, а як інтегральна складова інформаційної аналітики, здатна вплинути на бізнес-процеси, державні стратегії, оборонні системи та моделі наукових досліджень.

Метою роботи є аналіз сучасних підходів до комп'ютерної конкурентної розвідки із застосуванням технологій відкритої розвідки (OSINT), а також виявлення можливостей формалізації, систематизації та алгоритмізації процесів роботи з відкритими даними в умовах цифрової трансформації інформаційного простору.

Для досягнення поставленої мети визначено такі завдання дослідження:

– Проаналізувати сучасні наукові публікації та прикладні розробки у сфері OSINT як технології збору та аналізу інформації з відкритих джерел;

– Виявити ключові напрями розвитку комп'ютерної конкурентної розвідки з урахуванням сучасних інформаційних потоків;

– Запропонувати напрями подальшого наукового та прикладного розвитку OSINT як складової комп'ютерної конкурентної розвідки.

Виклад основного матеріалу дослідження

Аналіз наукових робіт котрі проходили під керівництвом Д. В. Ланде виявив системну методологію для комп'ютерної конкурентної розвідки, засновану на OSINT. Науковцями цієї групи було розроблено комплексну методику виявлення та прогнозування кіберінцидентів із застосуванням OSINT-інструментарію [9]. У роботі представлено повний цикл обробки інформації: від автоматизованого збору повідомлень через вебскрейпінг (зокрема, за допомогою Selenium WebDriver), до очищення текстів, побудови часових рядів динаміки публікацій, кластеризації тематичних потоків, а також виявлення іменованих сутностей (персон, організацій, геотегів) для семантичного аналізу.

Особливу увагу в дослідженні приділено валідації методології на реальному прикладі кібератаки на паливну інфраструктуру США Colonial Pipeline у травні 2021 року. Було зібрано та проаналізовано понад 1800 інформаційних повідомлень, що стосувалися цього інциденту, у період із 4 квітня по 12 червня 2021 року. На основі агрегованих даних було побудовано часовий ряд динаміки публікацій, який демонструє зростання обговорення в мережі у дні атаки, а також у фазі її наслідків.

Застосування вейвлет-аналізу з функцією MexH («мексиканський капелюх») дозволило виявити інформаційні аномалії у часовому ряді активну фазу атаки (6-12 травня) та фазу пост-фактум аналізу й обговорення (6-11 червня). Ці ділянки чітко візуалізуються на скейлограмі, що відображає щільність інформаційних сигналів у часі та масштабі (рис. 1).

Чітко виділяються дві фази: інцидент і суспільна реакція. Окрім того, автори використали модель прогнозування D. Sornette, яка базується на логарифмічно-періодичних коливаннях і дозволяє передбачати критичні точки інформаційного потоку, що можуть свідчити про наближення кіберінциденту. Застосування цієї моделі в рамках OSINT-підходу дозволяє не лише фіксувати факт атаки, а й прогнозувати її розвиток, ґрунтуючись на зміні патернів інформаційної активності.

Впровадження подібної методики в систему комп'ютерної конкурентної розвідки відкриває нові можливості для раннього виявлення критичних інформаційних змін, що

можуть вказувати на загрозу бренду, втрату репутації, появу конкурентних ризиків або інформаційно-економічних атак. Аналіз структури та динаміки інформаційних хвиль дозволяє розвідувальним системам не лише спостерігати за ринком постфактум, а прогнозувати інформаційні кризи або активність конкурентів у цифровому середовищі.

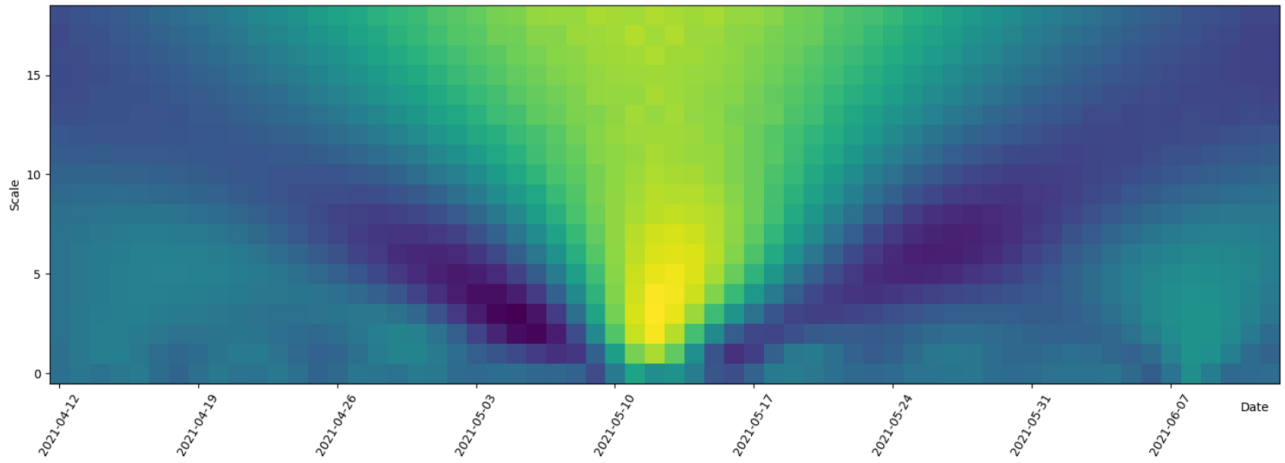

Рис. 1. Скейлограма часової динаміки повідомлень про атаку на Colonial Pipeline з використанням MexH-вейвлету (за [9, с. 212])

Інтеграція інструментів OSINT у конкурентну аналітику також забезпечує:

- моніторинг наративів у медіапросторі, пов'язаних із діяльністю компанії або її конкурентів;
- виявлення потенційно деструктивних інформаційних кампаній;
- географічну та персоніфіковану прив'язку інформаційних загроз;
- формування індикаторів репутаційної або стратегічної небезпеки.

Таким чином, методика, апробована на кейсі Colonial Pipeline, демонструє ефективність OSINT як інструменту не лише для кібербезпеки, а й для стратегічної бізнес-аналітики, що підвищує передбачуваність у конкурентному середовищі.

У праці за посиланням [10] було представлено архітектуру системи моніторингу соціальних медіа, що реалізує методологію аналізу інформаційних потоків у сфері кібербезпеки на основі поєднання технологій Big Data, Text Mining та OSINT-підходів. Автори Д. В. Ланде, І. В. Субач, О. С. Пучков описують багаторівневу систему, здатну працювати з великими масивами неструктурованих даних з таких відкритих джерел, як Telegram, Facebook, Twitter, YouTube, Reddit, а також з різноманітних веб-форумів та новинних агрегаторів.

Ключовими компонентами платформи є:

- модуль збору даних, який здійснює краулінг відкритих джерел;
- сховище великих даних, оптимізоване для роботи з потоками текстової інформації;
- система семантичного аналізу (Text Mining) для виявлення ключових сутностей: осіб, організацій, геотегів, тем;
- блок побудови часових рядів та вейвлет-аналізу, що дозволяє виявляти інформаційні аномалії;
- інструментальна панель візуалізації, яка дозволяє користувачеві отримати інтерактивний зріз інформаційного простору в реальному часі.

Особливу увагу в дослідженні приділено моделі виявлення пікових фаз інформаційного потоку за допомогою вейвлет-перетворення з базовою функцією "мексиканський капелюх" (MexH). Це дозволяє ефективно знаходити приховані закономірності у динаміці появи публікацій за певною темою. Наприклад, для запиту *«cybersecurity & coronavirus»* побудовано графік активності (рис. 8 у [10]), що демонструє дві фази інформаційного вибуху та поступового згасання інтересу.

Додатково система формує семантичні графи (рис. 6), які показують зв'язки між ключовими поняттями, організаціями, особами та географічними маркерами, що згадуються в потоці повідомлень. Це дає змогу не лише аналізувати контент за частотою, а й

будувати мережеву карту інформаційного впливу, яка може бути використана для виявлення джерел маніпулятивних кампаній, оцінки впливу ключових вузлів мережі (інфлюенсерів), а також формування сценаріїв подальшого розвитку інформаційної ситуації.

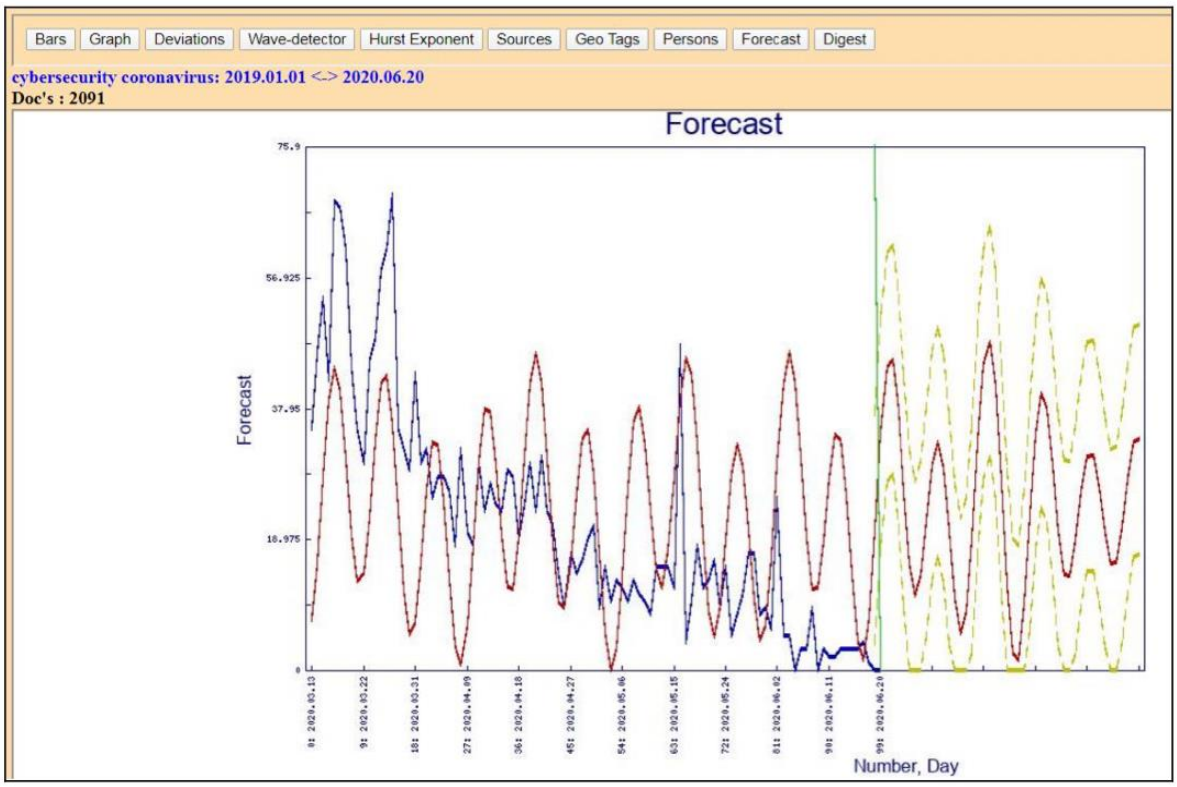

Рис. 2. Візуалізація динаміки повідомлень за темою «cybersecurity & coronavirus» у вигляді часової скейлограми з аномальними піками (за [10, с. 58])

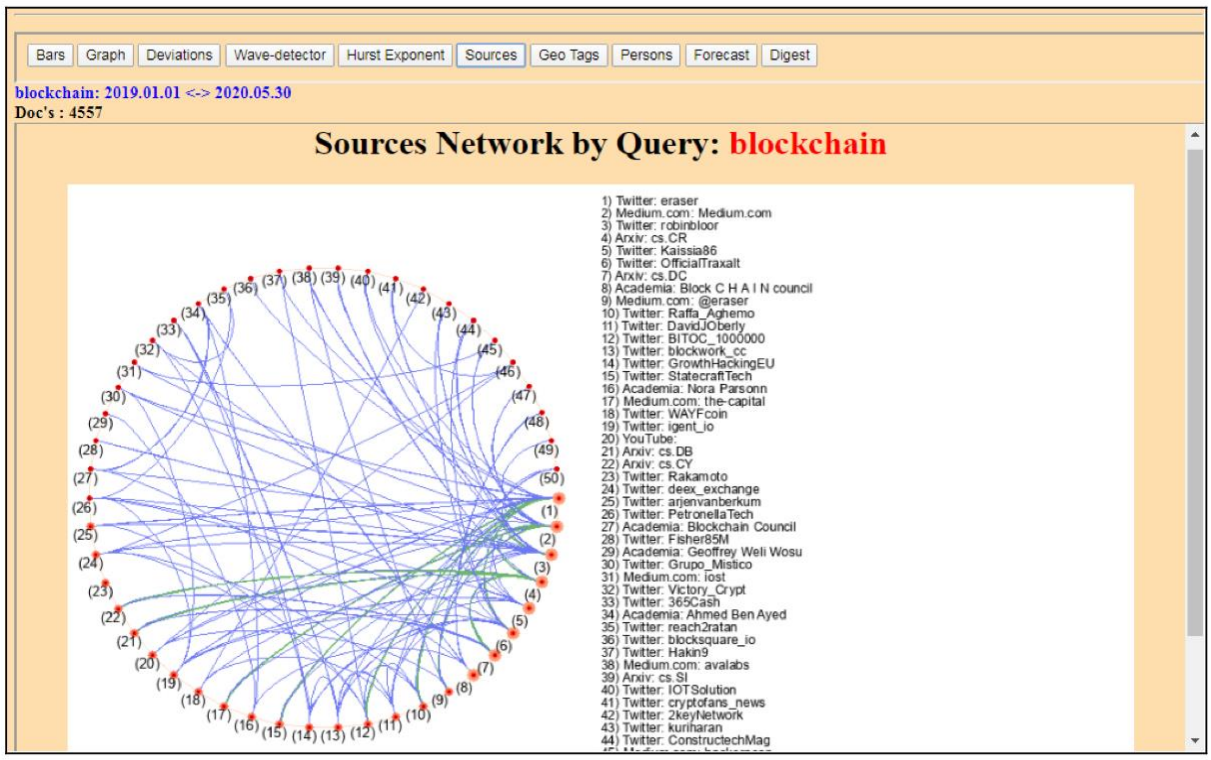

Рис. 3. Фрагмент семантичного графа, побудованого на основі аналізу ключових слів і сутностей у потоці повідомлень (за [10, с. 58])

Таким чином, описана система демонструє практичну реалізацію концепцій OSINT у сфері кібербезпеки й інформаційної аналітики та може бути інтегрована в інфраструктуру комп'ютерної конкурентної розвідки. Вона дає змогу оперативно виявляти репутаційні ризики, інформаційні загрози, поведінкові патерни аудиторій, що є критично важливим для стратегічного планування у бізнесі та державному секторі.

Фундаментальні підходи до використання OSINT як інструмента аналітики високого рівня були ґрунтовно викладені в монографії [11] «Розпізнавання інформаційних операцій: від нелінійного аналізу до прийняття рішень». У цій праці авторський колектив, під керівництвом Д. В. Ланде, сформував унікальне бачення OSINT не лише як засобу для збирання відкритої інформації, а як невід'ємного елементу складної системи інтелектуального аналізу. Концептуально технологія відкритої розвідки інтегрується в когнітивні, математичні та семантичні моделі, що здатні не просто фіксувати інформаційні явища, а виявляти закономірності, передбачати динаміку інформаційних процесів і генерувати обґрунтовані рішення.

Монографія пропонує глибоке осмислення інформаційних операцій як багатошарових процесів, в яких критичне значення має не лише сам обсяг інформації, а й структура, динаміка, вплив та взаємодія інформаційних вузлів. Особлива увага приділяється часовій природі інформаційних кампаній показано, як за допомогою вейвлет-аналізу можливо виявляти піки активності, фази зростання та спадання інформаційного тиску, а також прогнозувати настання переломних моментів у вигляді так званих точок біфуркації. У межах цієї аналітичної моделі інформація подається як потік, що має хвильову структуру і керується нелінійними законами розвитку.

У тексті розкривається роль семантичного аналізу у виявленні латентних смислів та зв'язків, які приховані у великих обсягах текстових повідомлень. За допомогою семантичного групування вдається не лише розкрити змістовне ядро інформаційної операції, а й ідентифікувати її ключові об'єкти, наративи та акторів. Побудовані когнітивні карти й семантичні графи виступають основою для розуміння структури впливу, формування інформаційних коаліцій, ідентифікації центрів координації деструктивного контенту.

Іншою важливою складовою дослідження є створення системи групової обробки даних і прийняття рішень у ситуаціях неповної визначеності. Запропоновані математичні конструкції на базі нечітких множин і матриць узгодження дозволяють враховувати експертні оцінки різного ступеня впевненості, що особливо важливо в аналізі інформаційних загроз у реальному часі.

Усі ці методологічні компоненти об'єднуються в єдину аналітичну платформу, що дає змогу обґрунтовано виявляти та оцінювати інформаційні впливи як на рівні окремих інцидентів, так і в масштабі системних інформаційних атак. Включення OSINT у цей комплекс дозволяє не лише збирати відкриту інформацію, а й наділяє її функціональністю – трансформує дані у знання, які можуть бути інтегровані у процеси кібербезпеки, державного управління або конкурентної бізнес-аналітики.

Особистий внесок Д. В. Ланде у цю роботу є фундаментальним. Він охоплює як розробку моделей виявлення інформаційних атак і системного представлення відкритих джерел, так і формалізацію термінологічної бази OSINT. Його напрацювання стали підґрунтям для створення прикладних рішень у сфері інформаційної безпеки, що успішно адаптуються до завдань стратегічного прогнозування, моніторингу ризиків і розвідки у конкурентному цифровому середовищі.

Сучасна парадигма комп'ютерної конкурентної розвідки формується в тісному зв'язку з розвитком відкритих цифрових джерел інформації, аналітичних методів і автоматизованих систем виявлення стратегічно важливих інформаційних патернів. Зокрема, значний вплив на структурування цього напряму справили праці Д. В. Ланде та його наукової школи, в яких розвідка розглядається не лише як технологія збору, а як інструмент когнітивної інтерпретації складних інформаційних потоків. У монографії «Розпізнавання інформаційних операцій: від нелінійного аналізу до прийняття рішень» [11] системно описано багаторівневу аналітичну

модель, що дозволяє виявляти інформаційні атаки та прогнозувати їхній розвиток на основі нелінійного аналізу. Саме ці положення стали підґрунтям для визначення ролі OSINT як аналітичного ядра конкурентної розвідки.

У працях [9], [10] автори пропонують прикладні підходи до побудови інформаційних систем аналізу потоків із відкритих джерел. Зокрема, у [9] представлено модель, що поєднує вебскрейпінг, часовий аналіз і кластеризацію з метою прогнозування кіберінцидентів, тоді як у [10] описано архітектуру системи для візуалізації соціальних інформаційних хвиль на основі інструментів Big Data та Text Mining. Саме ці системи й демонструють реальний перехід від збору до інтерпретації даних, що є ключовою рисою сучасної комп'ютерної конкурентної розвідки.

Теоретичну основу для визначення функціональних меж конкурентної розвідки як галузі закладено у монографіях [6] і [8], де розглянуто методи збору, обробки, а також обґрунтування допустимих меж застосування розвідувальних технологій у бізнесі та кіберсередовищі. Праця [7] містить важливе осмислення правових аспектівконкурентної розвідки, що дозволяє формувати етичні та процедурні рамки OSINT у корпоративному просторі.

Дослідження автоматичного виявлення основ подій інформаційних операцій [5] заклали підвалини для формування підходів до ранньої діагностики інформаційних загроз. Там обґрунтовано використання моделі Сорнета та когнітивних схем для оцінювання інтенсивності впливу. Ці механізми нині знаходять своє застосування у побудові систем стратегічного прогнозування в межах комп'ютерної конкурентої розвідки.

Актуальність підвищення цифрової компетентності фахівців у сфері OSINT яскраво підкреслюється в освітньому проєкті OSINT Academy [1], [2], який позиціонується як незалежна платформа для підготовки аналітиків нового покоління. Її створення та систематичне наповнення навчальними матеріалами свідчить про інституціоналізацію відкритої розвідки як легітимного інструменту конкурентної аналітики в Україні. Подібну роль у формуванні критичної маси дослідників відіграє й Інститут постінформаційного суспільства [3], [4], який зосереджується на взаємозв’язку інформаційної безпеки, цифрових прав і стратегічних інформаційних технологій, включаючи OSINT.

Таким чином, більшість наведених джерел є не лише фоновими, а й конструктивними: вони безпосередньо формують поле дослідження, забезпечують наукову доказовість використаних моделей, методик та інтерпретаційних стратегій. Посилання на них дозволяє забезпечити методологічну тяглість і продемонструвати обґрунтованість аналітичного висновку щодо еволюції комп'ютерна конкурентної розвідки у напрямі аналітико-прогностичного, цифрово-когнітивного та відкрито-семантичного підходу до розвідки.

У контексті формування нової цифрової епохи, що визначається домінуванням відкритих даних, багатовимірних інформаційних середовищ і стратегічного значення комунікаційного впливу, розвиток OSINT як складової комп’ютерної конкурентної розвідки вимагає переосмислення як наукового підходу, так і прикладної реалізації. Потреба в аналітичних інструментах, які дозволяють оперувати відкритою інформацією не фрагментарно, а системно, трансформує OSINT з механізму збору в повноцінну когнітивну технологію прийняття рішень.

Одним із ключових векторів подальшого наукового розвитку OSINT є побудова формалізованих моделей, що здатні об’єднувати різнорідні джерела даних у єдиний інформаційний простір. Це передбачає створення онтологічних структур, які б забезпечили уніфіковану інтерпретацію знань, отриманих із текстів, зображень, відео, метаданих і геопросторових об’єктів. Дотичним до цього постає завдання розробки алгоритмів семантичного узгодження, які б дозволяли синтезувати інформацію із різних платформ від урядових реєстрів і медіа до соціальних мереж у єдину аналітичну модель ситуації.

Також набуває дедалі більшого значення дослідження ролі штучного інтелекту у процедурі відкритої розвідки. Йдеться не лише про автоматизацію рутинних завдань (скрейпінгу, класифікації, фільтрації), а про здатність машинного навчання виявляти неочевидні взаємозв’язки, прогнозувати розвиток інформаційних подій та формувати аналітичні висновки в режимі реального часу. Саме у цьому полягає синергетичний потенціал

OSINT і AI як ядра нової генерації конкурентної розвідки, орієнтованої на аналітику не лише фактів, а й стратегій, мотивів, наративів.

У прикладному вимірі, перспективним напрямом розвитку є впровадження OSINT у сфери бізнес-аналітики, ринкового прогнозування, стратегічного планування та управління репутаційними ризиками. Комплексні платформи, що використовують OSINT як основу для візуалізації репутаційних змін, виявлення кампаній тиску або оцінки поведінкових трендів у споживчих спільнотах, вже доводять свою ефективність у корпоративному секторі. Розширення таких систем можливе за рахунок інтеграції з корпоративними системами управління знаннями, CRM та системами кіберзахисту.

Ще одним важливим напрямом є формування освітніх і професійних стандартів у галузі OSINT-аналітики. Відсутність єдиного етичного, правового і методологічного каркасу призводить до ситуації, коли технологічні можливості випереджають розуміння їхнього призначення та обмежень. Розвиток акредитованих програм підготовки фахівців із відкритої розвідки, сертифікаційних стандартів та етичного кодексу OSINT-аналітика є невід'ємною умовою професіоналізації галузі.

У стратегічній перспективі OSINT трансформується в інструмент не лише аналітичної підтримки, а й впливу на рівні інформаційних кампаній, антикризових стратегій і моделювання ризиків. Ця трансформація неможлива без поєднання знань з інформатики, прикладної лінгвістики, кібербезпеки, соціології й економіки. Таким чином, подальший розвиток OSINT як складової комп'ютерної конкурентної розвідки потребує мультидисциплінарної взаємодії, гнучких технологічних платформ і науково обґрунтованої методології.

Висновки

У результаті проведеного дослідження встановлено, що розвиток комп'ютерної конкурентної розвідки неможливий без глибокої інтеграції методології OSINT у структури аналітичного мислення сучасного цифрового суспільства. У статті було показано, що відкриті джерела інформації, які раніше сприймалися переважно як допоміжний інструмент, в умовах інформаційної перенасиченості перетворюються на самодостатній об'єкт аналітики, здатний генерувати знання стратегічного рівня. Це стало можливим завдяки поєднанню інструментів збору, структуризації, семантичної інтерпретації, когнітивного моделювання та нелінійного аналізу великих даних, що використовуються у сучасних наукових розробках, зокрема дослідницької школи Д. В. Ланде.

Важливою тезою, підтвердженою в статті, є трансформація OSINT із суто прикладної практики у повноцінну наукову дисципліну, що поєднує інформатику, лінгвістику, соціологію, психологію і економіку. Аналіз таких робіт, як монографія «Комп'ютерна конкурентна розвідка» (2021), дослідження інформаційних хвиль, а також архітектури систем обробки соціальних медіа, показує, що потенціал OSINT виходить далеко за межі оперативного збору даних. Саме в процесі формалізації та алгоритмізації інформаційних потоків реалізується аналітична потужність, здатна забезпечити адаптацію до кризових сценаріїв, прогнозування ризиків і виявлення інформаційних атак у зародку.

У цьому контексті наукова новизна полягає в обґрунтуванні концепції OSINT як ядра цифрової аналітики, що виконує роль об'єднуючої ланки між фактичним знанням і прийняттям управлінських рішень. Теоретичне значення дослідження полягає в закладенні основ багаторівневої моделі відкритої розвідки, орієнтованої на семантичну класифікацію, візуалізацію інформаційного тиску, а також когнітивне прогнозування, що розширює межі конкурентної розвідки як прикладної галузі. Практичний вимір дослідження відкриває шлях до створення гібридних систем підтримки рішень у бізнесі, безпеці, державному управлінні та антикризовому реагуванні.

Таким чином, OSINT у сучасному трактуванні – це не просто технологія, а структурна складова інформаційного суверенітету й стратегічної стабільності, що вимагає подальшого поглибленого міждисциплінарного осмислення та інституціонального впровадження.

Список використаної літератури:

1. OSINT Academy. (2024). Official website of the educational project on open-source. URL: https://osintacademy.com.

2. Zolotukhin, D. Y. (2016). (2016). OSINT Academy – educational materials from open sources. URL: https://www.youtube.com/@OSINTAcademy.

3. Public Organization "Institute of Post-Information Society". (2024). Official information from the Unified State Register. URL: https://youcontrol.com.ua/catalog/company_details/39954395/.

4. Institute of Post-Information Society. (2024). Official website of the public organization. URL: https://postinfosociety.com.

5. Lande D.V., Pryshchepa K.V. The automatic detection of the information operations event basis // *arXiv preprint arXiv:1807.03360*. 2018. URL: https://arxiv.org/abs/1807.03360.

6. Додонов А.Г., Ланде Д.В., Прищепа В. В., Путятин В. Г. *Комп'ютерна конкурентна розвідка*. – Київ: ТОВ «Інжиніринг», 2021. – 354 с.

7. Ланде Д. В. Правові питання конкурентної розвідки // *Інформація і право*. – 2020. – № 2. – С. 51–68.

8. Dodonov, A. H., Lande, D. V., Pryshchepa, V. V., & Putyatin, V. H. (2013). *Competitive Intelligence in Computer Networks*. Kyiv: NAS of Ukraine. 248 p.

9. Ланде Д.В., Пучков О., Субач І., Болюк М., Нагорний Д. OSINT-дослідження для виявлення та запобігання кіберінцидентам та атакам // *Інформаційні технології та безпека*. – 2021.–Т.9,№2. – С. 209–218. –URL:: https://its.iszzi.kpi.ua/article/view/249921/251241.

10. Ланде Д.В., Субач І., Пучков А. Система аналізу великих даних із соціальних медіа // Журнал інформаційної безпеки. – 2020. – Т. 47, № 1. – С. 44–61. URL: https://it4sec.org/system/files/4703_big_data_social_media.pdf.

11. Додонов А. Г., Ланде Д. В., Циганок В. О., Андрійчук О. Ю., Каденко С. О., Грайворонська А. М. Розпізнавання інформаційних операцій: від нелінійного аналізу до прийняття рішень: монографія. – Київ: ІПРІ НАН України, 2017. – 275 с.

Автори статті

Вишнівський Віктор – доктор технічних наук, професор, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0000-0003-1923-4344

Іщеряков Сергій – кандидат технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0007-5961-8218

Березовська Юлія – доктор філософії, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0000-0002-9973-0497

Термко Микита – магістр, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0008-8345-2171

Authors of the article

Vyshnivskyi Viktor – Doctor of Sciences (technical), Professor, State University of Information and Communication Technologies, Kyiv, Ukraine,

ORCID: 0000-0003-1923-4344

Ishcheryakov Serhii – Candidate of Sciences (technical), Associate Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0009-0007-5961-8218

Berezovska Yuliia – PhD, Associate Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0000-0002-9973-0497

Termko Mykyta – master, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0009-0008-8345-2171