Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет інфокомунікацій
(повна назва)

Кафедра інформаційно-мережної інженерії
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

Використання засобів пошуку та обробки інформації в мережі «Інтернет» в конкурентній розвідці

(тема)

Виконав:
здобувач 4 року навчання,
групи ТРІМІ-21-1
Світлана Гайова
(власне ім'я, прізвище)

Спеціальність 172 «Телекомунікації та радіотехніка»
(код і повна назва спеціальності)
Тип програми освітньо-професійна
Освітня програма Інформаційно-мережна інженерія
(повна назва освітньої програми)

Керівник доц. Вадим Золотарьов
(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри ІМІ _____ Валерій Безрук
(підпис) (власне ім'я, прізвище)

2025 р.

Не містить відомостей заборонених до відкритого публікування

Здобувач _____ / Гайова С.Б./

Керівник _____ / Золотарьов В.А./

Харківський національний університет радіоелектроніки

Факультет інфокомунікацій

Кафедра інформаційно-мережної інженерії

Рівень вищої освіти перший (бакалаврський)

Спеціальність 172 «Телекомунікації та радіотехніка»

Тип програми освітньо-професійна
(код і повна назва)

Освітня програма інформаційно-мережна інженерія
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
« 26» травня 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Гайової Світлані Борисовні
(прізвище, ім'я, по батькові)

1. Тема роботи Використання засобів пошуку та обробки інформації в мережі «Інтернет» в конкурентній розвідці

затверджена наказом університету від 26 травня 2025 р. № 410 Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії 18 червня 2025 р.

3. Вихідні дані до роботи Дослідити можливості використання інфокомунікацій в конкурентній розвідці підприємства, зокрема в мережі «Інтернет». З'ясувати які легальні джерела інформації про діяльність підприємства-конкурента можна знайти у відкритому доступі в мережі «Інтернет». Проаналізувати методи та засоби пошуку комерційної інформації та визначити їхню ефективність.

4. Перелік питань, що потрібно опрацювати в роботі

Вступ

1. Конкурентна розвідка: типи і особливості

2. Інформаційно – аналітичні аспекти конкурентної розвідки

3. Інтернет - розвідка

4. Метадані як джерело пошукових запитів

5. Порівняльний аналіз пошукових систем для КР

Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, кафедри)
Мета та напрями діяльності конкурентної розвідки, Різниця між конкурентною розвідкою та шпигунством, Розвідувально-аналітичні заходи, Складові кібернетичної розвідки, Пошук розвідувальної інформації в мережі «Інтернет», Етапи проведення інтернет-розвідки, Розвідувальний цикл та постановка задачі.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Ознайомлення із завданням. .	26.05.2025	виконано
2	Підбір джерел за темою роботи	27.05-29.05.2025	виконано
3	Написання першого розділу	30.05-01.06.2025	виконано
4	Написання другого розділу	02.06-04.06.2025	виконано
5	Написання третього розділу	05.06.2025	виконано
6	Написання четвертого розділу	06.06-07.06.2025	виконано
7	Написання п’ятого розділу	08.06-09.06.2025	виконано
8	Написання вступу та висновків	09.06.2025	виконано
9	Оформлення пояснювальної записки	10.06.2025	виконано
10	Подання пояснювальної записки на перевірку	16.06.2025	виконано

Дата видачі завдання 26 травня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ доц. Золотарьов В.А.
(підпис) (посада, власне ім’я, прізвище)

РЕФЕРАТ

Пояснювальна записка: - 57 с.,8 - рис.,4 - табл., 12 джерел, 2 додатки.

Мета роботи – дослідити особливості використання засобів пошуку та обробки інформації в мережі Інтернет для ефективного збору, аналізу та систематизації даних у процесі конкурентної розвідки, а також визначити оптимальні інструменти й методи для підвищення конкурентоспроможності підприємства.

Починається вона зі вступу в конкурентній розвідці. Далі розглядаються різні способи використання мережі “Інтернет” для пошуку та обробки даних у конкурентній розвідці.

Також особлива увага приділяється використанню Інтернету, інструментам інформаційно-комунікаційних технологій (ІКТ) загального призначення, інструментам ІКТ, адаптованим до одного або кількох етапів розвідки, а також інструментам бізнес-аналітики, включаючи сховища даних і інструменти для отримання та представлення даних. Нарешті, у розділі розглядаються різні способи, за допомогою яких організації можуть вибрати програми ІКТ для підтримки своєї розвідувальної діяльності.

КОНКУРЕНТНА РОЗВІДКА, ІКТ, ПОШУК ІНФОРМАЦІЇ, ІНТЕРНЕТ, АНАЛІЗ ДАНИХ, БІЗНЕС – АНАЛІТИКА, ІНСТРУМЕНТИ ІКТ

THE ABSTRACT

Explanatory note: 57 p., 8 - fig,4 - table,12 sources, 2 app.

The purpose of this work is to study the peculiarities of using the Internet search and information processing tools for efficient collection, analysis and systematisation of data in the process of competitive intelligence, and to identify the optimal tools and methods for improving the competitiveness of an enterprise.

It begins with an introduction to competitive intelligence. It goes on to consider various ways of using the Internet to search for and process data in competitive intelligence.

It also focuses on the use of the Internet, general-purpose information and communication technology (ICT) tools, ICT tools tailored to one or more phases of intelligence, and business intelligence tools, including data warehouses and tools for data retrieval and presentation. Finally, the section discusses the different ways in which organisations can choose to use ICT applications to support their intelligence activities.

COMPETITIVE INTELLIGENCE, ICT, INFORMATION RETRIEVAL, INTERNET, DATA ANALYSIS, BUSINESS ANALYTICS, ICT TOOLS

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ІБ – Інформаційна безпека;

ЗУ – Закон України;

ІКТ – Інфокомунікаційні технології;

КР – Конкурентна розвідка;

IMINT – Image Intelligence – розвідка за зображеннями;

OSINT – Open Source Intelligence – розвідка на основі відкритих джерел;

GEOINT – Geospatial Intelligence – г геопросторова розвідка;

SIGINT – Signals Intelligence – радіоелектронна розвідка;

HUMINT – Human Intelligence – агентурна розвідка;

CYBINT – Cyber Intelligence – кіберрозвідка;

SOCINT – Social Media Intelligence – розвідка за соціальними мережами;

FININT – Financial Intelligence – фінансова розвідка;

BINT – Business Intelligence – бізнес-розвідка.

ВСТУП

В умовах стрімкого розвитку цифрового простору ефективне управління бізнесом усе частіше залежить від здатності швидко отримувати, аналізувати та інтерпретувати зовнішню інформацію. Одним із ключових інструментів досягнення такої конкурентної переваги стає конкурентна розвідка, в основі якої лежить системний підхід до збору відкритих даних про ринок, конкурентів і споживачів. Використання інфокомунікаційних технологій значно розширює можливості цього процесу, підвищуючи його точність, оперативність та аналітичну глибину.

Застосування сучасних ІКТ дозволяє підприємствам у реальному часі отримувати доступ до великого обсягу різноманітної інформації, яка використовується для прийняття стратегічно важливих рішень. Наприклад, засоби штучного інтелекту та машинного навчання дають змогу автоматизувати пошук і класифікацію даних, виявляти тренди, моделювати сценарії розвитку подій на ринку. Аналітика соціальних мереж, зокрема інструменти аналізу настроїв користувачів, відкриває нові горизонти для розуміння споживчої поведінки та реакції на дії конкурентів.

Також варто відзначити зростання ролі хмарних платформ, які забезпечують мобільність, масштабованість та централізований доступ до інформаційних ресурсів. Це, в свою чергу, підвищує ефективність командної роботи аналітиків і дає змогу оперативно реагувати на зовнішні зміни.

Разом із технічними перевагами використання інфокомунікацій виникає і низка викликів, пов’язаних із дотриманням етичних стандартів, захистом персональних даних та забезпеченням інформаційної безпеки. Використання відкритих джерел потребує чітких правил щодо допустимості збирання та обробки інформації, особливо в контексті законодавчих вимог про захист даних.

У результаті можна стверджувати, що інфокомунікаційні технології стали невід’ємним інструментом сучасної конкурентної розвідки. Їх ефективне

впровадження сприяє зростанню аналітичних можливостей бізнесу, забезпечує глибше розуміння ринкових процесів та допомагає будувати довгострокові конкурентні стратегії. При цьому необхідно враховувати як технічні, так і етичні аспекти їх застосування, щоб уникнути ризиків і забезпечити сталий розвиток організації в конкурентному середовищі.

1 КОНКУРЕНТНА РОЗВІДКА: ТИПИ І ОСОБЛИВОСТІ

Конкурентна розвідка (КР) — це законний процес систематичного збору, обробки та аналізу відкритої інформації про конкурентів, ринкові тенденції та зовнішнє середовище. Ця інформація використовується для підтримки стратегічного й тактичного управління компанією. КР допомагає оцінити позицію компанії на ринку, оцінюючи ризики та можливості, діючи лише згідно з законом і моральними принципами. На відміну від цього, економічне шпигунство використовує незаконні методи, такі як втручання в інформаційні системи, підкуп працівників або крадіжка конфіденційних даних, що є незаконним і порушує мораль.

Основна ціль конкурентної розвідки полягає у зменшенні невизначеність у процесі прийняття управлінських рішень на рівні компанії, оцінити потенційні бізнес-можливості та виявити ризики та загрози, які впливають на діяльність підприємства. Вона охоплює оцінку репутації компанії в суспільстві, її партнерів, активів і доходів. При цьому вона уникає витоку конфіденційної чи персональної інформації, а також використання непрозорих джерел даних або методів характерних до оперативно-розшукової діяльності.

Щоб визначити роль і структуру конкурентної розвідки на корпоративному рівні, спочатку необхідно виявити види загроз для бізнесу, оцінити можливі збитки, а потім сформулювати мету створення відповідної служби, її завдання та інструменти для протидії та нейтралізації ризиків. Йдеться про запобігання будь-яким діям, подіям чи процесам, які можуть завдати шкоди діяльності компанії [1].

1.1 Мета конкурентної розвідки

Мета конкурентної розвідки полягає в тому щоб визначити у процесі прийняття управлінських рішень на корпоративному рівні та оцінити потенційні бізнес-можливості, виявити ризики і загрози які стосуються відповідно діяльності компанії, а також її публічної репутації, активів, доходів, бізнес-партнерів і тощо. При цьому уникнути витоку конфедеційної та персональної інформації, а також використання непрозорих джерел або методів оперативно-розшукової діяльності.

МЕТА КОНКУРЕНТНОЇ РОЗВІДКИ забезпечення ефективного реагування компанії на швидкі зміни навколишнього середовища і управління ризиками бізнес-діяльності через здійснення своєчасного інформаційно-аналітичного забезпечення процесу прийняття управлінських рішень	
Напрям діяльності	**Завдання**
Дослідження ринку (попит, пропозиція, ціни, тенденції, ноу-хау тощо) Вивчення та прогнозування нормативно-правового середовища	Збирання, аналіз і надання актуальної і достовірної інформації для прийняття рішень, своєчасне залучення уваги осіб, що приймають рішення, до потенційних загроз підприємницькій діяльності і запобігання їм, виявлення сприятливих можливостей для бізнесу
Вивчення конкурентів (стратегія, потенціал, орг., фінанс., тех. та ін. способи забезпечення конкурентних переваг тощо)	Виявлення і вивчення конкурентних переваг опонента(ів), їх копіювання та/або нейтралізація і відповідне коригування власної бізнес-стратегії
Вивчення діючих та потенційних партнерів (виробничі потужності, технології, фінансовий стан, репутація, ін.)	Оцінка ступеня вигідності умов співпраці з бізнес-партнерами, уникнення ділових відносин, запобігання загрозливим діям з боку несумлінних партнерів
Запобігання розвідувальній діяльності конкурентів	Виявлення слабких місць власної системи безпеки, виявлення спроб конкурентів незаконно отримати доступ до конфіденційної інформації компанії (у співпраці зі службою безпеки)

Рисунок 1.1 – Мета, напрями діяльності КР

1.2 Класифікація методів конкурентної розвідки

Використовуючи широкий спектр інструментів і методів, КР можна розділити на пасивні та активні. Пасивні методи включають збирання і аналіз відкритої інформації про ринок, галузь, законодавство, конкурентну компанію тощо з таких джерел, як мережа «Інтернет», друковані та електронні ЗМІ, офіційні документи компаній-конкурентів, а також метод «зворотної інженерії», тобто придбання та вивчення продуктів конкурентів. Активними методами є відвідування публічних заходів, таких як виставки, презентації та конференції; проведення підставних переговорів або наймання кандидатів на посади, а також проведення прихованих опитувань і робота з людьми, які можуть бути потенційними джерелами інформації [2].

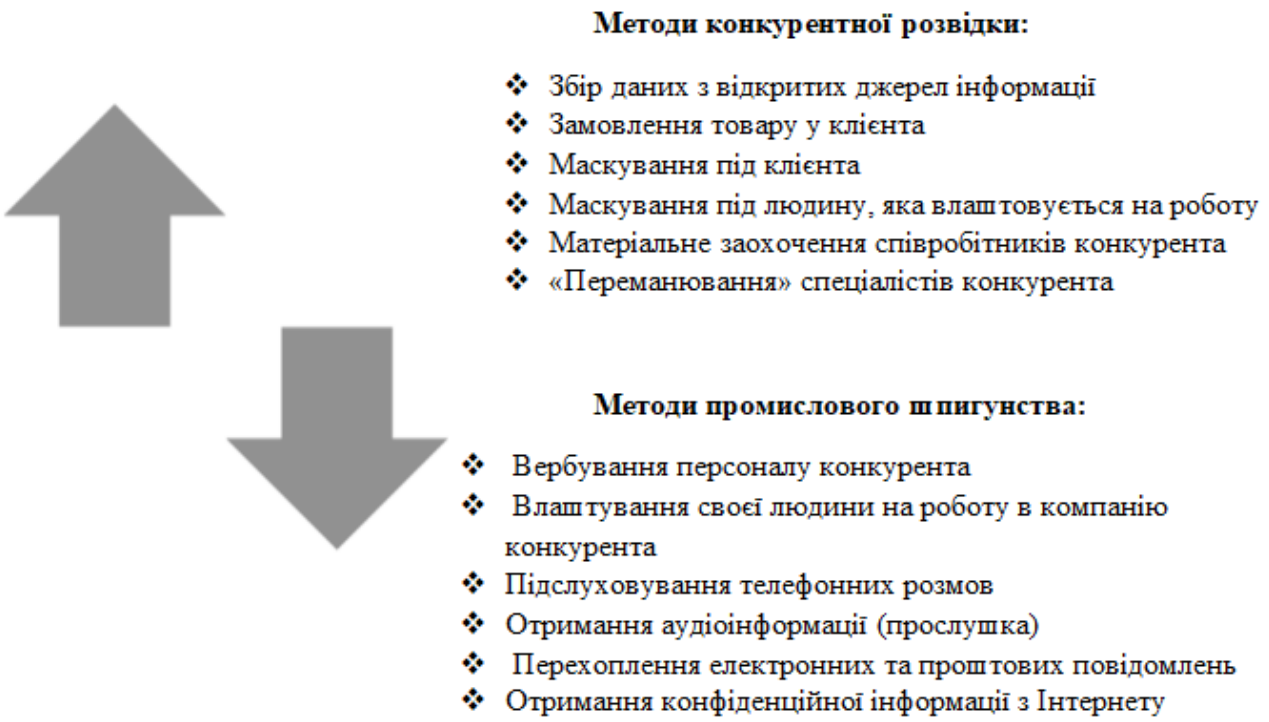

Рисунок 1.2 – Різниця конкурентної розвідки та промислового шпигунства

Представлений рис. 1.2 демонструє відмінності між методами конкурентної розвідки та методами промислового шпигунства, акцентуючи

увагу на межі між легітимною інформаційно-аналітичною діяльністю та незаконними діями, які порушують правові й етичні норми.

У верхній частині рисунка наведено методи, що належать до сфери конкурентної розвідки. Ці дії мають відкритий або умовно законний характер і включають використання публічної інформації, аналіз поведінки клієнтів, спостереження, а також так звані «сірі» практики, такі як замовлення товару або маскування під клієнта з метою отримання інформації про продукт чи сервіс конкурента. Також тут фігурують більш чутливі методи — наприклад, спроби переманити співробітників конкурента, що, попри моральні суперечки, за певних умов не суперечить закону.

У нижній частині схеми зображено методи промислового шпигунства, які є явно протиправними. До них належать: вербування співробітників з метою шпигування, нелегальне працевлаштування в компанії конкурента, підслуховування телефонних розмов, прослуховування приміщень, перехоплення електронної кореспонденції, а також незаконне отримання конфіденційної інформації з мережі «Інтернет». Такі дії становлять серйозне порушення як законодавства, так і принципів добросовісної конкуренції.

Стрілки між блоками символізують перехід від легітимних до нелегітимних практик, вказуючи на ризик, що діяльність, яка починається в рамках правового поля (наприклад, збирання відкритої інформації), за відсутності етичних стандартів та контролю може перерости у злочинну діяльність, тобто промислове шпигунство.

Таким чином, рисунок виступає наочною ілюстрацією тонкої межі між конкурентною розвідкою як частиною сучасного стратегічного менеджменту і протиправними діями, що підпадають під кримінальну відповідальність.

1.3 Типи конкурентної розвідки та їхні особливості

Конкурентна розвідка є багатогранним інструментом інформаційно-аналітичного забезпечення бізнесу, що

дозволяє підприємствам адаптуватися до динамічних умов ринкового середовища. Вона поділяється на кілька видів, кожен з яких має специфічні цілі, методи та напрями застосування.

На основі отриманою мною інформації зокрема у праці Юрія Когута можна виділити такі основні типи: стратегічна, тактична, технологічна, ринкова, а також кіберрозвідка [1].

Стратегічна конкурентна розвідка спрямована на довгострокове планування та формування конкурентних переваг компанії. Вона включає аналіз глобальних економічних тенденцій, політичних і законодавчих змін, а також оцінку стратегій ключових конкурентів. Основний напрям цієї розвідки — прогнозування змін у зовнішньому середовищі, що можуть вплинути на діяльність компанії, та оцінка потенційних можливостей для розширення бізнесу, наприклад, через вихід на нові ринки або створення партнерств. Особливістю цього виду є акцент на ретроспективному аналізі (розуміння минулих подій), перспективному прогнозуванні та проникливому осмисленні поточної ситуації, що дозволяє уникнути впливу суб’єктивних факторів на прийняття рішень.

Тактична конкурентна розвідка орієнтована на короткострокові операційні завдання. Її мета — оперативне реагування на дії конкурентів, зокрема через моніторинг їхньої цінової політики, маркетингових кампаній, змін у каналах збуту чи асортименті. Основний напрям діяльності — забезпечення менеджменту актуальною інформацією для швидкого коригування тактики компанії, наприклад, у відповідь на зниження цін конкурентами або запуск ними нових продуктів. Особливістю тактичної розвідки є її висока динамічність і залежність від своєчасного збору даних із відкритих джерел, таких як публічні звіти, реклама чи вебресурси конкурентів.

Технологічна конкурентна розвідка зосереджена на аналізі інноваційних розробок, патентів, ліцензій та інших результатів інтелектуальної діяльності. Вона дозволяє виявляти технологічні тренди, оцінювати потенціал нових розробок конкурентів і визначати можливості для власних інновацій. Основний напрям — захист інтелектуальної власності компанії та запобігання копіюванню її розробок, а також пошук можливостей для впровадження передових технологій у власне виробництво. Особливістю цього виду є необхідність використання спеціалізованих інструментів для аналізу патентних баз і технічної документації, а також залучення експертів із відповідних галузей.

Ринкова конкурентна розвідка фокусується на вивченні ринкового середовища, зокрема поведінки споживачів, змін у попиті та пропозиції, а також сегментації ринку. Її основний напрям — ідентифікація нових ринкових ніш, аналіз потреб клієнтів і прогнозування змін у їхніх уподобаннях. Цей вид розвідки допомагає адаптувати продукти чи послуги до потреб ринку, підвищуючи конкурентоспроможність компанії. Особливістю ринкової розвідки є її орієнтація на маркетингові аспекти, що вимагає використання методів сегментації ринку, аналізу конкурентного ландшафту та оцінки споживацьких трендів.

Кіберрозвідка є відносно новим видом конкурентної розвідки, що набуває актуальності в умовах зростання цифрових загроз. Вона включає моніторинг кіберпростору для виявлення потенційних ризиків, таких як хакерські атаки, витоки даних чи використання шкідливого програмного забезпечення. Основний напрям — забезпечення інформаційної безпеки компанії шляхом раннього виявлення загроз і прогнозування кібератак. Особливістю кіберрозвідки є її залежність від сучасних інформаційних технологій, зокрема використання спеціалізованих платформ, які дозволяють аналізувати великі обсяги даних із даркнету, відкритих джерел та інших каналів.

Таблиця 1.1 – Типи конкурентної розвідки

Тип розвідки	Спрямованість	Основні напрями	Особливості
Стратегічна	Довгострокові плани	Аналіз трендів, конкурентів, партнерів	Ретроспективний і прогнозний аналіз, об’єктивність
Тактична	Оперативні завдання	Спостереження за цінами, маркетингом	Оперативність, динамічність
Технологічна	Інноваційна діяльність	Дослідження патентів, нових технологій	Захист розробок, залучення спеціалістів
Ринкова	Ринкові умови	Аналіз сегментів, попиту	Фокус на маркетинг, орієнтація на клієнтів
Кіберрозвідка	Інформаційна безпека	Виявлення кіберзагроз, аналіз даркнету	Використання цифрових інструментів

Кожен із цих видів конкурентної розвідки має свої методи та інструменти, які застосовуються залежно від цілей компанії та специфіки її діяльності. Важливою умовою їх ефективного використання є дотримання етичних і правових норм, зокрема уникнення методів, що належать до оперативно-розшукової діяльності, та використання лише відкритих джерел інформації.

1.4 Етичні та правові аспекти конкурентної розвідки

Конкурентна розвідка (КР) є ефективним інструментом для надання бізнесу інформаційно-аналітичної допомоги, її успіх значною мірою залежить від дотримання етичних стандартів. З метою забезпечення легітимності бізнесу, запобігання репутаційним ризикам і підтримки довіри з боку клієнтів, партнерів і суспільства були розроблені етичні стандарти КР. Як зазначає SCIP, конкурентна розвідка має базуватися на моральних принципах, таких як дотримання законодавства, використання виключно відкритих джерел інформації та повагу до прав інших [1].

Основні етичні принципи КР включають:

– прозорість методів збирання інформації: фахівці з КР повинні використовувати лише легальні та етичні методи, такі як аналіз відкритих джерел (вебсайти, публікації, звіти), участь у публічних заходах чи опитування, що не порушують конфіденційність [1]. Наприклад, неприпустимо представлятися іншою особою для отримання інформації чи використовувати методи, що межують із промисловим шпигунством;

– дотримання конфіденційності**:** КР не передбачає розкриття конфіденційних даних компаній чи осіб без їхньої задокументованої згоди. Це включає уникнення використання "сірих" баз даних або інформації, отриманої незаконним шляхом [3];

– чесність у представленні результатів: Аналітики КР повинні надавати об’єктивну та достовірну інформацію, уникаючи маніпуляцій чи спотворення даних для досягнення бажаних висновків [1]. Це забезпечує довіру до результатів розвідки з боку керівництва компанії;

– повага до конкурентів: тична КР виключає дії, що можуть завдати шкоди репутації чи бізнесу конкурентів, наприклад, поширення дезінформації чи "чорного піару" [1];

Етичні стандарти також гарантують, що конфлікти інтересів не виникають. Наприклад, фахівець із КР не може одночасно працювати на конкуруючій компанії, якщо це може призвести до розкриття конфіденційної інформації. Дотримання етичних принципів сприяє розвитку професійної репутації та зменшує ризик судових позовів чи втрати довіри клієнтів [1].

Для забезпечення легітимності КР і захисту від звинувачень у незаконній діяльності важливе правове регулювання. В Україні та по всьому світу КР регулюється різними законами, що регулюють інформаційну діяльність, захист персональних даних, комерційну таємницю та боротьбу з недобросовісною конкуренцією.

1.4.1 Міжнародне законодавство

На міжнародному рівні КР регулюється правилами, що стосуються захисту комерційної таємниці, персональних даних та інтелектуальної власності. Наприклад, Загальна правила захисту даних (GDPR), які регулюють збор, обробку та зберігання персональних даних, діють у Сполучених Штатах і країнах ЄС [4]. Порушення цих правил може призвести до великих штрафів і втрати репутації. Крім того, міжнародні стандарти, такі як кодекси SCIP, рекомендують уникати методів, які можна розглядати як промислове шпигунство, таких як несанкціонований доступ до корпоративних мереж або підкуп співробітників [1].

1.4.2 Українське законодавство

В Україні правові аспекти КР регулюються низкою законів, зокрема:

Закон України "Про захист персональних даних": цей закон встановлює вимоги до збору та обробки персональних даних, забороняючи їх використання без згоди суб’єкта. Наприклад, КР не може включати аналіз персональних даних, отриманих із нелегальних джерел, таких як "злиті" бази даних [5].

Закон України "Про захист від недобросовісної конкуренції": цей закон забороняє дії, що можуть бути кваліфіковані як недобросовісна конкуренція, зокрема, неправомірне отримання комерційної таємниці чи її розкриття [6]. Фахівці з КР повинні уникати методів, що можуть порушувати цей закон, наприклад, використання інсайдерської інформації.

Закон України "Про захист інформації в інформаційно-комунікаційних системах": цей закон регулює захист інформації в IT-системах, забороняючи несанкціонований доступ до даних компаній чи осіб [7].

Кримінальний кодекс України: статті, що стосуються незаконного збирання, зберігання чи поширення конфіденційної інформації, можуть застосовуватися до випадків, коли КР переходить межу законності, наприклад, при використанні методів промислового шпигунства [8].

Для легітимності та ефективності конкурентної розвідки важливі етичні та правові аспекти. Прозорість, чесність і повага до конфіденційності забезпечують довіру бізнес-спільноти до КР. З метою захисту діяльності КР від промислового

шпигунства законодавство як в Україні, так і за кордоном обмежує її [9]. Тим не менш, необхідно продовжувати вдосконалювати нормативну базу та підвищувати моральну свідомість фахівців через проблеми, пов’язані з новими технологіями, відсутністю чіткого законодавства та низькою правовою культурою. Для розвитку КР як стратегічного інструменту бізнесу важливим є забезпечення балансу між ефективністю та дотриманням моральних і правових стандартів.

2 ІНФОРМАЦІЙНО – АНАЛІТИЧНІ АСПЕКТИ КОНКУРЕНТНОЇ РОЗВІДКИ

Інформаційно-аналітичні аспекти цієї діяльності базуються на системному зборі, обробці та аналізі інформації про зовнішнє середовище підприємства, зокрема про конкурентів, ринок, інновації та технології. Особливу роль у цьому процесі відіграють цифрові технології, що забезпечують доступ до відкритих джерел, автоматизацію обробки великих обсягів даних і підвищення точності аналітики. У цьому розділі розглянуто основні види розвідувальної діяльності, методи збору інформації та сучасні підходи до її аналізу в межах конкурентної розвідки.

2.1 Види розвідувальної діяльності

В країнах НАТО розрізняють шість видів розвідувальної діяльності.

Розвідка з відкритих джерел (OSINT) – це інформація, яка є публічно доступною та з’являється з джерел, які не мають ніякої таємності або обмежень доступу [10].

Найстаріший спосіб збору інформації від її носіїв – агентурна розвідка (HUMINT) [10].

Видова розвідка (IMINT) — це відтворення об’єктів на плівці, електронних дисплеях або інших носіях [10].

Радіоелектронна розвідка (SIGINT) — це перехоплення сигналів між людьми, машинами або обома [10].

Інструментальна розвідка (MASINT)— це розвідка електромагнітних полів, яка збирає наукові та технічні дані для визначення, виявлення та опису специфічних ознак для конкретних цілей [10].

Геопросторова розвідка (GEOINT) — це процес створення зображень і геопросторових даних за допомогою інтеграції географічних даних і зображень місцевості [10].

Рисунок 2.1 – Перетинання розвідувально-аналітичних дисциплін

Використання відкритих джерел інформації (OSINT), яке включає публічні дані в мережі «Інтернет», офіційні звіти, наукові публікації та соціальні мережі, є важливим компонентом сучасної конкурентної розвідки. Цей метод є легальним, моральним і широко застосовується в бізнес-середовищі завдяки доступності та ефективності інфокомунікаційних технологій.

Через етичні, правові та технічні перешкоди інші методи розвідки, такі як агентурна (HUMINT), видова (IMINT), радіоелектронна (SIGINT), інструментальна (MASINT) і геопросторова (GEOINT), можуть бути або неприйнятні для використання в конкурентній розвідці, або їх не можна використовувати. Зокрема, HUMINT може застосовуватися лише в контексті легітимних контактів і відкритих інтерв'ю. Інші методи, такі як збирання сигналів за допомогою спеціалізованих сенсорів або аналіз геолокаційних даних, не дозволені в цивільному бізнес-середовищі.

2.2 Методи конкурентної розвідки

Пасивні методи — передбачають збирання інформації з відкритих джерел, зокрема: офіційних вебсайтів, публікацій у ЗМІ, соціальних мереж, аналітичних баз даних. Ці методи активно використовують інфокомунікаційні технології та мережу “Інтернет”, оскільки інформаційний пошук, обробка даних і моніторинг відбуваються у цифровому середовищі.

Активні методи — охоплюють дії з безпосереднього отримання інформації через взаємодію з джерелом: участь у виставках, переговорах, проведення опитувань. Хоча основний акцент не робиться на цифрові технології, деякі інструменти — такі як електронна пошта чи відеозв’язок — можуть застосовуватись на практиці.

Інтернет-розвідка (Internet intelligence) — є самостійною групою методів, повністю орієнтованих на онлайн-середовище. Вона охоплює моніторинг відкритих джерел (OSINT), використання веб-аналітики, обробку великих обсягів даних. Цей напрямок тісно пов’язаний з інформаційними системами, пошуковими алгоритмами та ІКТ.

Технологічна розвідка — спрямована на аналіз інновацій, патентного середовища, науково-дослідної активності конкурентів. Тут також активно застосовуються інформаційні технології, особливо під час пошуку та обробки інформації в спеціалізованих цифрових базах.

Аналітичні методи — охоплюють інструменти стратегічного аналізу, такі як SWOT, GAP-аналіз, конкурентні матриці та бенчмаркінг. Попри те, що вони самі по собі є методологічними підходами, інформація для їх реалізації здобувається через ІКТ або мережу “Інтернет”.

Таблиця 2.1 - Методи конкурентної розвідки та застосування ІКТ

Методи конкурентної розвідки	Застосування ІКТ	Застосування мережі «Інтернет»	Характеристика
Пасивні методи	Так	Так	Активно використовують інфокомунікаційні технології та мережу «Інтернет» для цифрового пошуку та обробки даних
Активні методи	Так	Ні	Основний акцент не на цифрові технології, застосовуються лише окремі ІКТ-інструменти
Інтернет-розвідка	Так	Так	Повністю орієнтовна на онлайн-середовище, тісно пов’язана з ІКТ
Технологічна розвідка	Так	Так	Активне застосування інформаційниї технологій для пошуку та обробки інформаціїї в цифрових базах
Аналітичні методи	Так	Так	Самі методи є методлогічними підходами, але інформація для реалізації здобувається через ІКТ або Інтернет

Таким чином, можу зробити висновок, що більшість сучасних методів конкурентної розвідки так чи інакше інтегровані з цифровими технологіями. Найбільш технологічно залежними виявились інтернет-розвідка та пасивні методи, які майже повністю функціонують у цифровому середовищі та базуються на використанні інформаційно-комунікаційних технологій та мережевих ресурсів [1].

2.3 Аналіз методів розвідки

Розвідку кібернетичного простору супротивника (у нашому випадку підприємства-конкурента) можна умовно поділити на розвідку інфокомунікаційних систем та комп’ютерну розвідку (розвідку інформаційних систем)

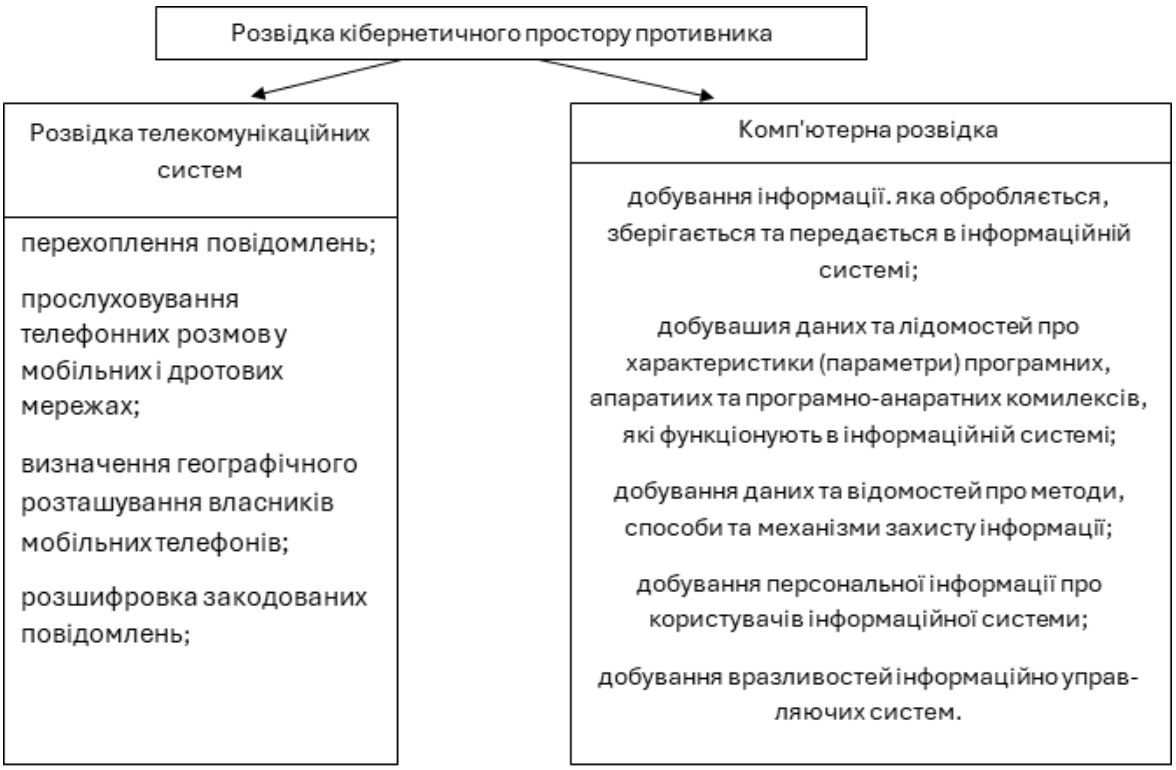

Рисунок 2.2 – Складові кібернетичної розвідки

Перехоплення повідомлень і прослуховування розмов у мобільних і дротових мережах, визначення географічного розташування власників телефонів і розшифровка закодованих повідомлень є методами конкурентної розвідки в бізнесі, які вважаються неприйнятними через їх неетичну природу, незаконність і відхилення від принципів використання відкритих джерел інформації. Це суперечить законодавству, зокрема нормам, що регулюють захист персональних даних і оперативно-розшукову діяльність. Це також порушує етичні стандарти, які підтримують подібні практики. Визначення, де знаходяться власники телефонів, може розглядатися як вторгнення в особисте життя, що суперечить стандартам бізнес-розвідки.

Крім того, розшифровка закодованих повідомлень є незаконною. Це не відповідає легальним методам збору даних, які традиційно базуються на доступних джерелах, таких як медіа чи публікації, які містять значну частину необхідної інформації. Застосування таких методів може призвести до юридичних ризиків, таких як кримінальна відповідальність, а також дошкодити

репутації компанії. Це суперечить меті конкурентної розвідки, яка полягає в забезпеченні безпеки бізнесу та ефективного управління. Для бізнес-розвідки краще використовувати етичні та законні методи, такі як аналіз відкритих даних, спостереження за соціальними мережами, бенчмаркінг і прогнозування тенденцій, які відповідають правовим і моральним нормам.

Методи комп’ютерної розвідки наведені на рис.2.3.

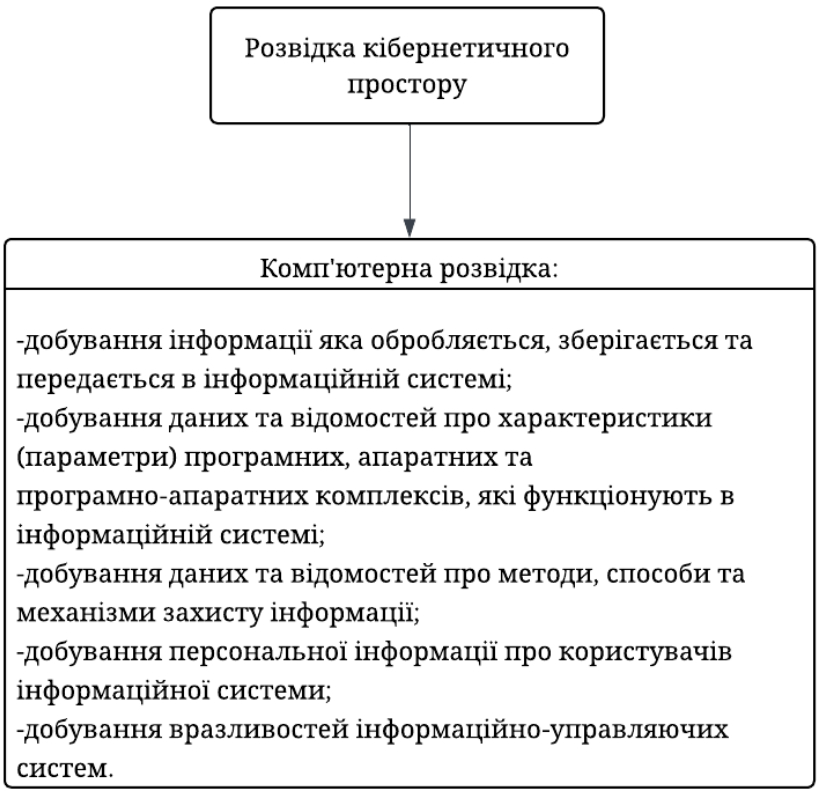

Рисунок 2.3 – Аналіз методів розвідки інформаційних систем

Добування інформації, яка обробляється, зберігається та передається в інформаційних системах, узгоджуються з основною частиною кібернетичної розвідки. Ця частина кібернетичної розвідки включає комп’ютерну розвідку, яка передбачає отримання даних із засобів електронно-обчислювальної техніки та глобальних мереж, і служить основою для планування наступальних кібер Процес сканування мережі, відомий як віддалений аналіз хостів, використовується для збору даних про характеристики програмних, апаратних і

програмно-апаратних комплексів. Цей процес дозволяє визначити перелік відкритих портів і атакуючих додатків, а також виявити активні служби та ймовірні шляхи атак. Розвідка кібернетичних загроз пов’язана з отриманням відомостей про методи захисту інформації.

Розвідка кібернетичних загроз включає систематизацію даних про потенційні джерела загроз, що дозволяє виявляти слабкі місця за допомогою апаратно-математичного моделювання атак. Незважаючи на те, що персональна інформація користувачів не є найважливішою, соціальна інженерія допомагає пасивним методам розвідки ідентифікувати ключових осіб у системах противника. Нарешті, добування вразливостей інформаційно-управляючих систем узгоджується з активним аналізом і скануванням. Це дозволяє попереджати кібернетичний вплив на інформаційно-комунікаційні мережі, збираючи початкові дані про об’єкти впливу.

Усі методи були розділені на два підрозділи. Перший включав комп’ютерну розвідку, яка зосереджувалася на вразливостях через сканування технічних даних, а другий — розвідку кібернетичних загроз, яка аналізує захисні механізми та персональні дані для виявлення джерел загроз. Таким чином, методи комп’ютерної розвідки інтегруються з підходами кібернетичної розвідки, що сприяє підвищенню ефективності розвідувальних заходів у кібернетичному просторі для забезпечення національної безпеки. Вважається, що комбінація пасивних і активних підходів є найкращим способом оцінити як їхні переваги, так і недоліки.

3 ІНТЕРНЕТ - РОЗВІДКА

Інтернет-розвідка є ключовим інструментом у структурі сучасної конкурентної розвідки. Вона полягає в цілеспрямованому зборі, обробці, верифікації та аналізі інформації, що розміщена у відкритому доступі в мережі ”Інтернет”. Ряд дослідників визначають цей різновид розвідки як аналітичне опрацювання великих обсягів інформації з множини відкритих джерел, що дозволяє виявити цінні дані для прийняття стратегічних рішень.

Сутність інтернет-розвідки полягає не лише у пошуку інформації, а й у її структурованій передачі, перевірці достовірності та подальшому аналітичному опрацюванні. Це дозволяє створювати релевантні інформаційні продукти для підтримки управлінських рішень [11].

3.1 Структура інтернету як середовища розвідки

Особливістю інтернету як джерела розвідувальної інформації є його дворівнева структура:

- видимий інтернет – частина мережевого контенту, доступна для індексації стандартними пошуковими системами. За різними оцінками, він охоплює лише 20–30% загального обсягу інформації в мережі. Деякі джерела наводять цифру до 50% [4];
- Невидимий або глибинний Інтернет – сукупність ресурсів, які не індексуються пошуковими машинами. Доступ до них можливий лише за умови знання адреси або спеціального доступу. Це можуть бути бази даних, внутрішні документи, тендерні архіви, технічна документація тощо [4].

Таким чином, значна частина потенційно цінної інформації для КР не знаходиться у відкритій видачі пошукових систем, що зумовлює необхідність застосування спеціальних методів доступу до глибинних ресурсів.

Організація пошуку розвідувальної інформації в мережі «Інтернет» показано на рис. 3.1.

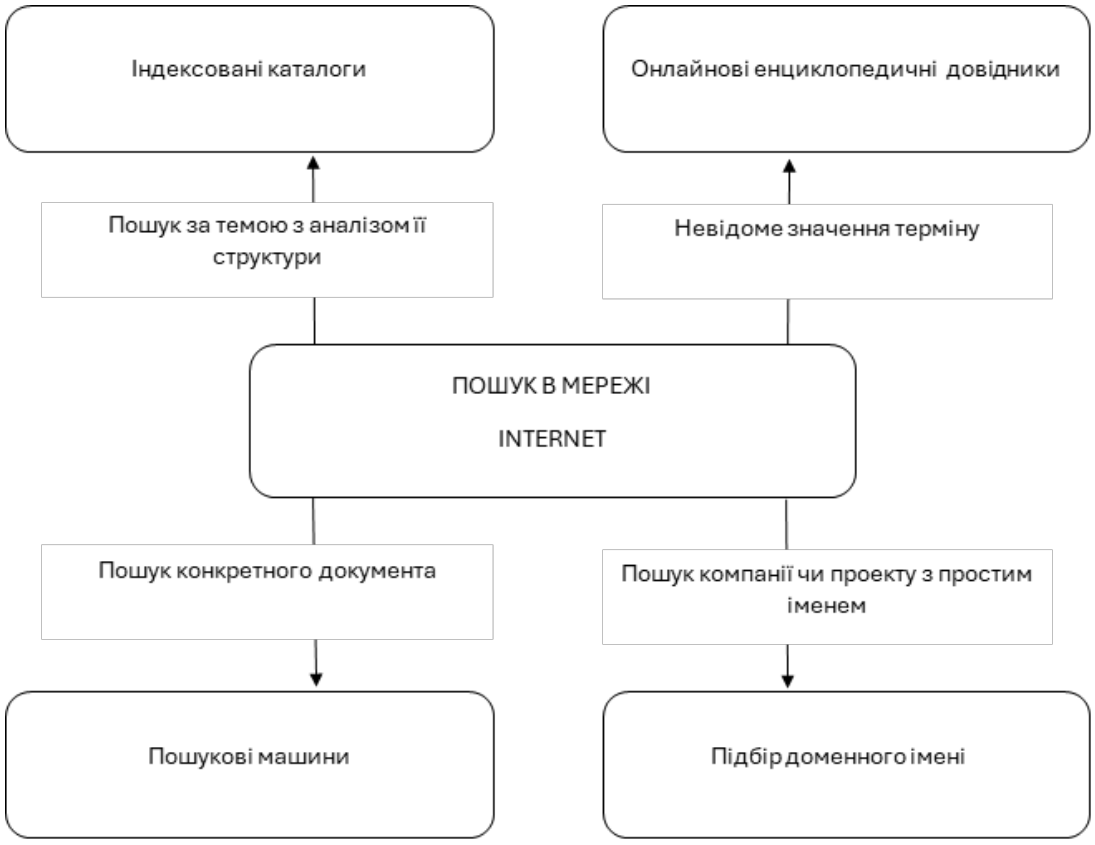

Рисунок 3.1 -Пошук розвідувальної інформації в мережі «Інтернет»

3.2 Особливості доступу до інформаційних ресурсів у мережі «Інтернет»

Процес ефективної інтернет-розвідки являє собою складну багаторівневу діяльність, що ґрунтується на чіткій послідовності етапів, кожен з яких забезпечує цілісність та результативність аналітичного дослідження. У межах конкурентної розвідки інтернет-розвідка відіграє особливо важливу роль, оскільки дозволяє з високим ступенем актуальності отримувати інформацію про ринкове середовище, конкурентів, споживчі настрої та потенційні загрози інформаційній безпеці [1].

Рисунок 3.2 ілюструє основні етапи організації процесу інтернет-розвідки, починаючи з формування запиту і закінчуючи побудовою аналітичного звіту. Представлений ланцюг дій відображає загальні підходи до структурованого пошуку, обробки та верифікації інформації в межах конкурентної розвідки.

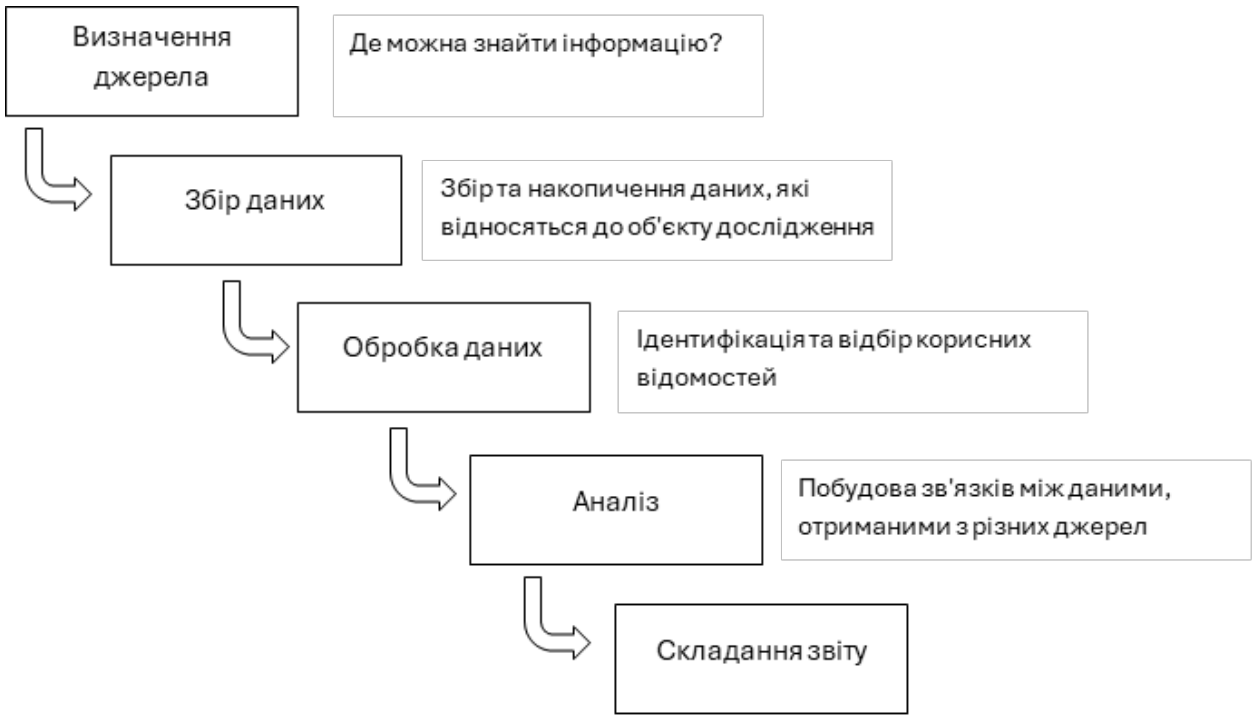

Рисунок 3.2 – Етапи проведення інтернет-розвідки

Першим критично важливим етапом є постановка інформаційного завдання, що передбачає формулювання цільового вектора розвідки, чітке визначення об’єкта спостереження, специфікацію запитуваної інформації та встановлення параметрів релевантності. Успішна постановка завдання гарантує, що всі подальші дії будуть орієнтовані на досягнення аналітичного результату, максимально наближеного до потреб управлінського процесу [1].

Наступним логічним кроком є формування запиту, що вимагає застосування відповідних операторів пошуку. До таких належать логічні модифікатори (AND, OR, NOT), уточнення контексту за допомогою лапок, знаків мінусів, а також фільтрів за часом, типом файлу чи доменною зоною. Саме формування коректного запиту визначає глибину і точність інформаційного

охоплення. Ефективність даного етапу значною мірою залежить від обізнаності фахівця у синтаксисі пошукових систем та практиці так званого «інформаційного глибокого занурення» (deep search) [1].

Третій етап — вибір інструментів пошуку та обробки даних, що включає як традиційні пошукові системи (Google, Bing, DuckDuckGo), так і спеціалізовані ресурси: наукові агрегатори (Google Scholar, Semantic Scholar), відкриті бази даних, бізнес-реєстри, ресурси OSINT, цифрові архіви (Wayback Machine) тощо. В окремих випадках доцільним є використання інструментів пасивного збору даних (наприклад, WHOIS, Maltego), соціальних інженерних платформ або агрегаторів аналітичного моніторингу [1].

Після отримання початкових результатів здійснюється первинний аналіз інформації, що охоплює експертну оцінку джерел, перевірку їх авторитетності, встановлення ступеня актуальності, достовірності та формальної відповідності до інформаційного запиту. Важливу роль на цьому етапі відіграє ідентифікація фейкових або маніпулятивних даних, а також виявлення вторинних або дубльованих джерел [1].

Далі здійснюється систематизація отриманих даних, що передбачає їх структурування, архівацію у базу знань або систему аналітичної звітності. Важливим аспектом є формування уніфікованих категорій, що дозволяє у майбутньому здійснювати порівняльний аналіз та ретроспективний огляд тенденцій [1].

Наступним етапом виступає аналітична обробка, яка включає верифікацію отриманих даних, виявлення повторів і суперечностей, тематичну класифікацію, побудову логічних моделей взаємозв’язків, а також формування синтезованих висновків щодо тенденцій і потенційних сценаріїв розвитку досліджуваного об’єкта. Аналітична обробка передбачає не лише описовий, але й прогностичний рівень, що особливо актуально в умовах динамічного конкурентного середовища [1].

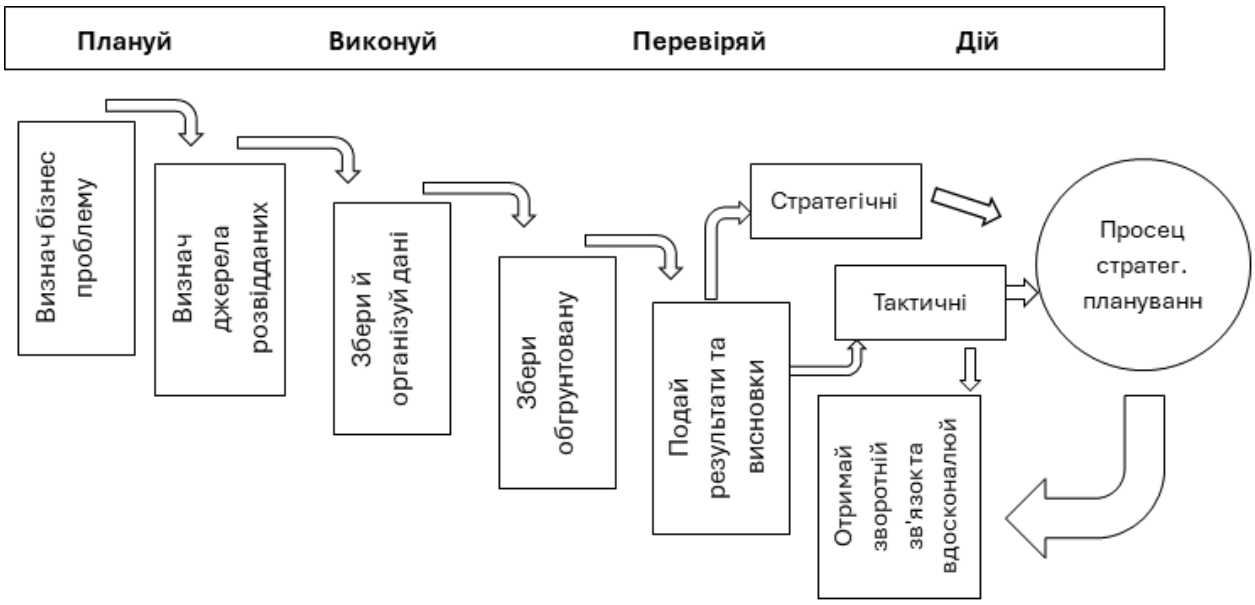

Рисунок 3.3 – Розвідувальний цикл та постановка задачі

Підвищення ефективності інтернет-розвідки досягається за рахунок поєднання традиційного пошукового підходу з інструментами автоматизованого моніторингу, новинними агрегаторами, системами збирання цифрових слідів (digital footprint tracking), платформами семантичного аналізу, штучного інтелекту та машинного навчання. Такий інтегрований підхід забезпечує глибоку обробку даних, підвищує швидкість реагування на зміну інформаційного середовища та дозволяє реалізовувати інформаційно-аналітичну підтримку прийняття управлінських рішень на стратегічному рівні.

3.3 Класифікація та відбір джерел інформації для конкурентної розвідки

Найбільш поширеним та динамічним джерелом інформації у сфері конкурентної розвідки є мережа Інтернет, яка забезпечує доступ до широкого спектра безкоштовних онлайн-ресурсів. До таких ресурсів належать корпоративні сайти, офіційні публікації, електронні ЗМІ, блоги, вікі-платформи, аналітичні портали та соціальні медіа (зокрема LinkedIn, Twitter, Facebook). Інтернет також слугує каналом для отримання структурованих даних із

відкритих державних реєстрів, електронних торговельних майданчиків, галузевих баз знань і комерційних інформаційних систем [1].

Окрім цифрових джерел, значну аналітичну цінність мають первинні канали отримання інформації, зокрема контакти зі співробітниками компаній, клієнтами, галузевими експертами, партнерами, постачальниками, учасниками конференцій і членами професійних асоціацій. Такі джерела дозволяють отримати контекстуалізовану, емпірично підтверджену інформацію, що не завжди відображається у відкритих публікаціях [1].

У зв’язку з надмірною кількістю потенційно доступних джерел виникає необхідність у системному підході до їх відбору. Вибір джерел має базуватися на низці об’єктивних критеріїв, зокрема оперативності доступу до інформації, ступеня надійності ресурсу, точності, актуальності й можливості верифікації даних. При цьому важливо, щоб процес відбору не знижував цінності отриманої інформації та не призводив до викривлення аналітичних висновків.

Інформаційні потреби конкурентної розвідки є надзвичайно різноплановими та охоплюють як загальні організаційно-фінансові характеристики, так і технологічні, маркетингові та кадрові аспекти діяльності конкурентів [1].

4 МЕТАДАНІ ЯК ДЖЕРЕЛО ПОШУКОВИХ ЗАПИТІВ

Метадані є основним джерелом для побудови пошукових запитів, а також для визначення змісту документів і оцінки їх контексту та значущості. Опрацювання метаданих — це стратегічний спосіб захисту інформації для бізнесу, оскільки це дозволяє компанії правильно позиціонуватися в конкурентному середовищі, прогнозувати ризики та приймати розумні управлінські рішення. У цьому підрозділі розглядаються різні види метаданих, які використовуються під час пошуку бібліографічної інформації про конкурентів, способи її пошуку та інструменти цифрової обробки в мережі “Інтернет”.

4.1 Аналіз основних метаданих для пошуку бібліографії

Однією з ключових умов ефективної конкурентної розвідки в системі забезпечення інформаційної безпеки підприємства є здатність швидко знаходити, аналізувати та використовувати метадані, такі як структуровані відомості про джерела інформації, їх зміст, авторство, структуру та технічні параметри, є важливим компонентом ефективної конкурентної розвідки в системі забезпечення інформаційної безпеки підприємства. У процесі пошуку інформації метадані служать навігаційним інструментом, щоб знайти бібліографію конкурентів, їхню діяльність, публікації та патентні дії, участь у тендерах, конференціях або парі.

В основі цієї діяльності лежить систематичне використання відкритих джерел інформації та спеціалізованих засобів пошуку та обробки інформації в мережі “Інтернет” . Ці методи забезпечують як первинний збирання даних, так і подальший аналіз зв’язків, фактів, подій, учасників, ризиків і можливостей [2].

Метадані використовуються для побудови ефективних пошукових запитів і виявлення інформаційних слідів конкурентів у відкритому інформаційному

просторі. У контексті конкурентної розвідки, яка є складовою інформаційної безпеки підприємства, виділяють кілька ключових груп метаданих:

– тематичні ключові слова: конкурентна розвідка; інформаційна безпека; захист інформації; бізнес-аналітика; комунікаційні технології [2];

– галузеві терміни: системи захисту інформації; кібербезпека підприємств; управління ризиками; аналітичне забезпечення; інформаційно-аналітичний супровід [2];

– організаційні метадані: назви компаній-конкурентів; установчі документи; внутрішня документація; звітність; тендерні матеріали [2];

– персональні метадані: імена керівників та фахівців; контактна інформація; професійні біографії; публікаційна активність [2].

Для реалізації ефективного бібліографічного пошуку в межах конкурентної розвідки застосовуються як пасивні, так і активні методи. До пасивних методів належать: аналіз відкритих джерел; моніторинг ЗМІ; дослідження офіційних документів; зворотна інженерія. Активні методи включають: участь у публічних заходах; проведення опитувань та інтерв'ю; встановлення ділових контактів; мережевий аналіз професійних зв'язків.

Значне місце у реалізації таких завдань займає "Інтернет"-середовище, де представлена як офіційна інформація, так і другорядні цифрові сліди діяльності компаній. Згідно з науковими дослідженнями, в мережі "Інтернет" у відкритому вигляді можна виявити лише 10–15 % релевантної інформації. Решта 85–90 % потребує глибшої обробки, порівняння, систематизації та аналітичного осмислення з використанням відповідного програмного забезпечення [2].

У науковій літературі та прикладних дослідженнях виділяються такі групи засобів пошуку й обробки інформації в мережі "Інтернет":

– базові засоби пошуку: пошук на окремих сайтах; підбірки посилань; каталоги; пошукові та метапошукові системи;

– аналітичні засоби: системи моніторингу; контент-аналізу; екстрактори подій і фактів; системи Text Mining; Data Mining; Knowledge Discovery [2];

– спеціалізовані системи: програмні рішення конкурентної розвідки, що поєднують інструменти пошуку, інтеграції, аналізу та візуалізації даних [2].

При побудові запитів важливо дотримуватись такої структури: основна тематика — "конкурентна розвідка" + "інформаційна безпека"; галузеві уточнення — "комунікаційні технології" + "захист даних"; організаційний контекст — назва компанії + "стратегія безпеки"; персональний рівень — ім’я експерта + "публікації" + "дослідження".

Джерела розвідувальних даних класифікуються на:

– людські ресурси: експерти; працівники конкурентів; свідки подій; учасники професійних спільнот;

– матеріальні об’єкти: зразки продукції; виставкове обладнання; технічні макети; рекламні матеріали;

– документальні джерела: установчі документи; технічна документація; рекламні публікації; звіти органів влади;

– цифрові ресурси: вебсайти компаній; соціальні мережі; електронні бази даних; системи електронного документообігу.

Для досягнення високого рівня достовірності та ефективності пошуку рекомендується комбінувати методи; систематично оновлювати пошукові запити; перевіряти інформацію з кількох джерел; дотримуватись етичних стандартів; застосовувати спеціалізовані програмні засоби [2].

Таким чином, системний аналіз метаданих у поєднанні з ефективними методами та цифровими інструментами пошуку дозволяє виявляти релевантну бібліографічну інформацію про конкурентів і посилювати інформаційно-аналітичну безпеку підприємства у стратегічному вимірі.

4.2 Кластерний аналіз цифрових слідів у конкурентній розвідці

У цифрову епоху кожна взаємодія користувача з інформаційними системами залишає за собою так звані цифрові відбитки — сліди дій, що зберігаються у журналах активності, мережевому трафіку, сесійних даних або зовнішніх аналітичних платформах. Такі сліди можуть містити відомості про час і спосіб доступу до ресурсу, поведінкові особливості користувача, його інтереси, взаємодії з контентом тощо. Саме цей тип інформації дедалі активніше використовується в аналітичних цілях, зокрема в межах конкурентної розвідки.

У разі аналізу зовнішньої або напіввідкритої цифрової інфраструктури організацій-конкурентів (наприклад, корпоративних порталів, хмарних платформ, систем підтримки клієнтів) можна отримати непрямі відомості про те, як поводяться внутрішні чи зовнішні користувачі, як часто оновлюються сервіси, які підрозділи є найбільш активними тощо. Наприклад, аналіз періодичності змін документації, повторюваних звернень або публікацій у відкритих каналах може вказувати на функціональну активність певного напряму компанії.

Одним з ефективних методів обробки такої інформації є кластерний аналіз, який дає змогу згрупувати користувачів або інформаційні події за подібними характеристиками. Це дозволяє структурувати великі обсяги неструктурованих даних та виділити типові моделі поведінки. Відповідно до сучасних досліджень, користувачі цифрових середовищ можуть класифікуватися за рівнем обізнаності у сфері інформаційної безпеки.

До основних типів користувачів належать:

– обізнані користувачі – демонструють високий рівень цифрової культури, дотримуються вимог інформаційної безпеки, активно відстежують оновлення політик, використовують багатофакторну автентифікацію, не залишають надмірних слідів у цифровому просторі [12];

– неуважні або недбалі користувачі – нехтують базовими вимогами безпеки, використовують слабкі паролі, можуть працювати через незахищені пристрої, не оновлюють програмне забезпечення своєчасно [12];

– неінформовані користувачі – не мають достатнього рівня знань щодо сучасних кіберзагроз, можуть бути мішенню фішингових атак або стати учасниками витоку інформації через власну необережність [12];

– байдужі користувачі – ігнорують системні повідомлення, не реагують на інциденти безпеки, не зважають на наслідки своїх дій у цифровому середовищі [12];

– безвідповідальні користувачі – навмисно порушують правила внутрішньої політики, користуються несанкціонованими засобами обміну інформацією, зберігають конфіденційні документи в загальнодоступних середовищах [12];

– деструктивні користувачі – мають намір завдати шкоди інформаційній системі, діють усвідомлено, можуть бути мотивовані внутрішніми конфліктами або зовнішнім впливом (наприклад, з боку конкурентів чи зловмисників) [12].

З погляду конкурентної розвідки, виявлення публічної активності представників компанії-конкурента (наприклад, на форумах, у відкритих техпідтримках, у коментарях до документації, у професійних соціальних мережах) може слугувати основою для непрямої ідентифікації типу користувача та рівня його ризику. Якщо користувач демонструє відкритість до обговорення внутрішніх процедур або несвідомо розкриває специфіку технологій компанії, це створює потенційно вразливий канал для збору розвідданих.

Наприклад, недбалі працівники можуть випадково публікувати службову інформацію у відкритих чатах, коментарях до презентацій або у публічних резюме. Безвідповідальні користувачі можуть залишити посилання на внутрішні ресурси або обговорювати проблеми корпоративної безпеки на зовнішніх платформах. Навіть обізнані фахівці іноді розкривають опосередковані ознаки внутрішніх проєктів, коли публікують статті або дописи про свою роботу.

У контексті конкурентної розвідки такий підхід дозволяє не лише зрозуміти загальну структуру цифрової взаємодії в компанії-конкуренті, а й виокремити потенційні "слабкі місця" в її інформаційній архітектурі. Наприклад, якщо компанія активно використовує публічну CRM-систему або має відкритий

API-інтерфейс, можна дослідити шаблони дій зареєстрованих користувачів: час доступу, частоту оновлень, географію IP-адрес. Це дає змогу зробити висновки про внутрішню структуру бізнес-процесів або взаємодію підрозділів [12].

Практичний приклад: під час спостереження за публічною технічною базою даних IT-компанії-конкурента виявлено, що в періоди оновлень з’являються нові облікові записи, які залишають великі обсяги коментарів щодо тестування продуктів. З аналізу цифрових слідів можна припустити, що ці користувачі є внутрішніми тестувальниками або субпідрядниками. Така інформація дозволяє дізнатися про графік розробки, рівень залучення зовнішніх фахівців і навіть оцінити інтенсивність роботи над продуктом.

Загалом, кластеризація цифрових слідів може стати ефективним інструментом для непрямої оцінки інформаційної гігієни організації, виявлення патернів потенційно ризикованої поведінки та прогнозування точок уразливості. Важливо підкреслити, що всі дії з обробки подібних даних повинні здійснюватися в межах чинного законодавства та етичних стандартів, без порушення конфіденційності або неправомірного доступу до захищених систем.

4.3 Аналіз засобів пошуку та обробки інформації в мережі «Інтернет»

Для професійних цілей вибір пошукової системи повинен базуватись на низці критичних технічних та функціональних показників, які забезпечують якість і надійність результатів пошуку:

– релевантність результатів – здатність алгоритму пошуку адекватно інтерпретувати контекст запиту та формувати максимально точну видачу;

– швидкість індексації – оперативність відображення нових вебресурсів і публікацій у результатах пошуку;

– повнота індексу – обсяг охоплення джерел, типів контенту та структури вебпростору;

– персоналізація – здатність адаптувати результати під користувача без надмірного втручання у об'єктивність пошуку;

– захист приватності – обсяг даних, які система збирає, та принципи їх подальшого використання;

– стійкість до маніпуляцій – надійність фільтрації неякісного або шкідливого контенту;

– мобільна оптимізація – ефективність роботи інтерфейсу пошукової системи на смартфонах і планшетах;

– наявність розширених функцій – підтримка голосового пошуку, пошуку за зображенням, фільтрації за атрибутами.

За даними глобального огляду (2023–2025), частки пошукових систем розподіляються таким чином - Google утримує домінування з часткою понад 91 %, Bing – близько 3 %, Baidu та DuckDuckGo – до 2 %. Незважаючи на високу популярність Google, функціональні переваги альтернативних систем дозволяють їх використовувати в певних сферах.

Google виділяється серед конкурентів завдяки масштабній базі даних, що перевищує 100 петабайт, впровадженню передової технології MUM для обробки складних багаторівневих запитів та глибокій інтеграції з екосистемою Google Workspace, що забезпечує безперебійну роботу в корпоративному середовищі.

Bing досягає значних результатів у сфері візуального та мультимедійного пошуку, використовуючи потужність штучного інтелекту GPT-4 та тісну взаємодію з продуктами Microsoft, що робить його особливо привабливим для користувачів корпоративних рішень.

DuckDuckGo позиціонується як захисник приватності користувачів, повністю відмовляючись від створення персональних профілів та відстеження активності, водночас пропонуючи зручну систему швидкого пошуку через !bangs команди для миттєвого доступу до конкретних ресурсів.

З метою підвищення ефективності інформаційного пошуку в межах завдань конкурентної розвідки доцільно застосовувати логічні оператори та модифікатори формулювання запитів. Серед базових технік варто виокремити наступні:

– використання лапок для формулювання "точної фрази", що забезпечує пошук повного лексичного збігу;

– застосування знака мінус (–) для виключення певних слів або термінів із результатів видачі;

– оператор site: дозволяє обмежити пошук матеріалами в межах конкретного домену;

– filetype: призначений для фільтрації результатів за типом файлу (наприклад, pdf, doc, ppt);

– команда intitle: орієнтує пошук на наявність ключового слова безпосередньо в заголовках сторінок.

Окрім базових прийомів, ефективність підвищується шляхом використання розширених параметрів: операторів альтернативності (наприклад, OR для синонімів), часових обмежень (діапазони дат через подвійні крапки), географічної специфікації запитів, а також уточнень через фахову термінологію або контекстні атрибути.

5 ПОРІВНЯЛЬНИЙ АНАЛІЗ ПОШУКОВИХ СИСТЕМ ДЛЯ КР

У сучасному інформаційному середовищі роль пошукових систем як інструменту збору, верифікації та аналізу інформації є надзвичайно важливою для реалізації завдань конкурентної розвідки. Пошукові системи забезпечують оперативний доступ до відкритих джерел інформації (OSINT), включаючи вебсайти організацій, наукові публікації, соціальні мережі, документи державних установ, новинні стрічки, спеціалізовані бази даних тощо.

Згідно з даними дослідження, від 10 до 15% стратегічно корисної інформації знаходиться у прямому доступі в мережі Інтернет, решта ж потребує додаткової аналітичної обробки, інтеграції та порівняння. Саме тому ефективне використання пошукових систем із підтримкою спеціалізованих функцій пошуку, операторів, фільтрів та інструментів інтелектуального аналізу є критичним фактором успішної реалізації КР [11, 12].

5.1 Критерії ефективності пошукових систем

Для об'єктивної оцінки пошукових систем у сфері конкурентної розвідки виділено такі ключові критерії:

– Релевантність результатів – наскільки точно відповідає видача поставленому запиту;

– Глибина індексації – обсяг та різноманіття проіндексованих джерел;

– Швидкість оновлення – як швидко нові сторінки потрапляють до індексу;

– Функціональність – підтримка операторів логічного пошуку (filetype:, site:, intitle:);

– Конфіденційність – політика приватності та обмеження збору персональних даних;

– Зручність для користувача – інтерфейс, фільтрація, доступність мобільної версії.

Таблиця 5.1 - Порівняльна характеристика Google, Bing і DuckDuckGo

Критерій	Google	Bing	DuckDuckGo
Релевантність результатів	Дуже висока	Висока	Середня
Глибина індексації	Найвища	Висока	Помірна
Оновлення контенту	Майже в реальному часі	Швидке	Помірне
Оператори пошуку	Повний набір	Підтримуються частково	Частково
Пошук файлів (PDF, DOC)	Так	Так	Обмежено
Персоналізація	Висока (через обліковий запис)	Середня	Відсутня
Конфіденційність	Низька	Середня	Висока
Інтерфейс	Зручний, інтегрований	Чистий, з AI Copilot	Мінімалістичний

Google утримує позицію лідера тому що вирізняється швидкою індексацією новинного та професійного контенту, а також підтримкою розширених пошукових інструментів, таких як Google Lens, Google Dataset Search і Google Scholar. Низька конфіденційність пошукової активності користувача залишається головним недоліком.

Коли Bing інтегрувався з інструментами штучного інтелекту (GPT-4), він став придатним для глибшого аналітичного пошуку, особливо щодо академічних і професійних потреб.

Незважаючи на те, що його видачі не такі точні, DuckDuckGo є безпечним і приватним інструментом пошуку. Він не зберігає особисті дані, тому може використовуватися в ситуаціях, коли анонімність під час розвідки є важливою.

5.2 Практичне тестування: приклад порівняння результатів

З метою практичного підтвердження теоретичних положень щодо ефективності пошукових систем у завданнях конкурентної розвідки було здійснено тестування за однаковим інформаційним запитом у різних пошукових платформах.

Тестовий запит "бізнес-аналітика конкурентів в IT-сфері Україна 2024" filetype:pdf

Цей запит є релевантним до завдань КР, оскільки передбачає пошук актуальних PDF-документів, що містять аналітичну інформацію про конкурентів у галузі інформаційних технологій в Україні.

Мета: Оцінити релевантність, кількість результатів, точність фільтрації PDF-документів.

Платформи для порівняння: Google, Bing, DuckDuckGo

Таблиця 5.2 – Порівняльні результати

Пошукова система	Кількість релевантних результатів	Чітке застосування фільтру filetype:pdf	Загальний вміст результатів	Коментар
Google	7	Так	Аналітичні звіти, презентації, публікації організацій	Найвища точність та актуальність
Bing	6	Частково	Наукові PDF, комерційні звіти	Результати схожі на Google, але з меншою релевантністю
DuckDuckGo	4	Частково	Слабка фільтрація, змішані формати	Переважають застарілі документи

Результати підтверджують перевагу використання Google для виконання інформаційних запитів у конкурентній розвідці, яка вимагає точного фільтрування за типом документу та високого рівня релевантності. Bing може бути корисним інструментом для допомоги, особливо якщо ви можете отримати

доступ до контенту Microsoft. DuckDuckGo обмежен в використанні через слабку фільтрацію та наукову вузькість.

Практичний експеримент підтвердив доцільність комбінованого підходу: використання кількох пошукових платформ із різними профілями дозволяє аналітику розширити інформаційну базу при збереженні релевантності даних.

ВИСНОВКИ

У процесі дослідження теми «Використання засобів пошуку та обробки інформації в мережі “Інтернет” в конкурентній розвідці» було досягнуто поставлену мету. Мета полягала в тому, щоб детально описати процеси, інструменти та джерела інформації, які застосовуються в сучасній інтернет-розвідці в контексті аналітики конкурентів. З’ясувалося, що конкурентна розвідка, що базується на відкритих джерелах, є законною інформаційно-аналітичною діяльністю і відіграє стратегічну роль у забезпеченні безпеки бізнесу. Вона дотримується моральних і правових стандартів, що відрізняє її від промислового шпигунства.

Інтернет є основним середовищем для конкурентної розвідки, оскільки він надає доступ до великої кількості відкритих і умовно відкритих джерел, таких як бази даних, соціальні медіа, корпоративні сайти та цифрові архіви. Інтернет-розвідка виконується як послідовність етапів, починаючи з планування інформаційного завдання та закінчуючи аналітичною обробкою та інтерпретацією зібраних даних. Верифікація інформації – це перевірка її достовірності, надійності, актуальності та унікальності. Це важливий компонент ефективності. За допомогою цифрових слідів і метаданих можна розширити аналітичний потенціал розвідки, виявляючи непрямі ознаки та характеристики джерел. Порівняльний аналіз пошукових систем показав, що Google є найефективнішим інструментом загального пошуку. З іншого боку, спеціалізовані системи, такі як Google Scholar, працюють добре з науковими даними. Отже, інтернет-розвідка є однією з ключових компетенцій інформаційного суспільства, а її ефективність зумовлена поєднанням методичної точності, технологічного інструментарію та розвиненого аналітичного мислення користувача.

ПЕРЕЛІК ПОСИЛАНЬ

1. Когут Ю. Конкурентна розвідка та безпека бізнесу: практичний посібник. Київ : Сідкон, 2021.

2. Мужанова Т. М. Конкурентна розвідка як інструмент інформаційно-аналітичного супроводу забезпечення інформаційної безпеки підприємства. Економіка і суспільство. 2018. Т. 16. С. 7.

3. Ланде Д. В. Правові питання конкурентної розвідки. Інформація і право. 2020

4. Леонова Ю. О. Міжнародний досвід використання конкурентної розвідки. Економіка, фінанси, право. 2017.

5. Про захист персональних даних : ЗУ від 01.06.2010, № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/236/96-вр#Text.

6. Про захист від недобросовісної конкуренції : ЗУ від 07.06.1996, № № 236/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/236/96-вр#Text.

7. Про захист інформації в інформаційно-комунікаційних системах : ЗУ від 05.07.1994, № № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/main/80/94-вр#Text..

8. Кримінальний кодекс України : ЗУ від 05.04.2001, № № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

9. Березіна Л., Братанов Б. Характерні особливості конкурентної розвідки та промислового шпигунства підприємств. Інтелект XXI. 2020. С. 6.

10. Цифрова розвідка на основі відкритих джерел (Частина I). PSD info. Розвідка. 25.12.2022. URL: https://www.psdinfo.pro/post/

11. Ємельянов С. Комп'ютерна розвідка як особливий різновид технічної розвідки. Сучасна спеціальна техніка. 2012.№1.

12. Кластерний аналіз дослідження цифрових слідів студентів закладів освіти / В. Лахно та ін. Кібербезпека: освіта, наука, техніка. 2024. Т. 3, вип. 21. С. 31–41. URL: https://doi.org/10.28925/2663-4023.2024.23.3141.