Київський столичний університет імені Бориса Грінченка Факультет інформаційних технологій та математики Кафедра комп'ютерних наук

**«Допущено до захисту»** Завідувач кафедри комп'ютерних наук
доктор технічних наук, професор
**(науковий ступінь, наукове звання)**
Бондарчук А.П.
**(прізвище, ініціали) (підпис)**
« ___» _____2025р.

**КВАЛІФІКАЦІЙНА РОБОТА**
**на здобуття освітнього ступеня «Магістр»**
**Спеціальність 122 Комп'ютерні науки**
**Освітня програма 122.00.02 Інформаційно-аналітичні системи**

# Тема роботи «Практичне використання штучного інтелекту для проведення OSINT - досліджень»

**Виконав**
студент групи _ІАСм-1-24-1.4д_____
**(шифр академічної групи)**
Курсеітов Олександр Олександрович
**(прізвище, ім'я, по батькові)**
_____
**(підпис)**
**Науковий керівник**
_доктор технічних наук, професор._
**(науковий ступінь, наукове звання)**
_Бушма Олександр Володимирович_
**(прізвище, ініціали)**
_____
**(підпис )**

Київ – 2025

Київський столичний університет імені Бориса Грінченка

Факультет інформаційних технологій та математики

Кафедра комп'ютерних наук

**«Затверджую»** Завідувач
кафедри комп'ютерних наук,
кандидат технічних наук, доцент
(науковий ступінь, наукове звання)

Машкіна І. В. _____
(прізвище, ініціали)(підпис)

« ____»_____2024_ р.

# ЗАВДАННЯ НА ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

**студенту групи** _ІАСм-1-24-1.4д_____

Курсеітов Олександр Олександрович

(прізвище, ім'я, по батькові)

**Тема роботи: Практичне використання штучного інтелекту для проведення OSINT - досліджень**

1. Вихідні дані: відкриті джерела інформації (соціальні мережі, новинні ресурси, онлайн- реєстри), інструменти OSINT і ШІ (LLM-моделі, сервіси геолокації, інструменти аналізу зображень та відео), тестові кейси для проведення OSINT-досліджень.
2. Основні завдання проаналізувати сучасний стан розвитку OSINT та застосування ШІ; виконати класифікацію ШІ-інструментів для OSINT; розробити комплексну методику інтеграції ШІ в OSINT-цикл; реалізувати прототип ШІ-асистента та випробувати його на практичних кейсах; оцінити ефективність запропонованих рішень і сформувати практичні рекомендації.
3. Пояснювальна записка: Обсяг – до 86 стор. формату А4 комп'ютерного набору з дотриманням вимог стандарту і методичних рекомендацій кафедри.
4. Графічні матеріали: презентація.

5. Додатки: схематичне зображення схем системи, зображення додатку та фрагменти програмного коду.

6. Строк подання роботи на кафедру:

Науковий керівник
к.т.н., доцент

_____О. В. Бушма

Завдання прийняв до виконання
«___» _____20__р.

_____
(підпис студента)

# АНОТАЦІЯ

Магістерська робота: 86 с., 16 рис., 10 табл., 51 джерело.

**Актуальність:** робота присвячена практичному використанню інструментів ШІ в OSINT-дослідженнях за умов зростання обсягів відкритих даних і дезінформації.

**Об'єкт дослідження:** процеси збору, обробки та інтерпретації відкритої інформації в OSINT-системах.

**Предмет дослідження:** методи, моделі та інструменти ШІ для підвищення ефективності OSINT-досліджень і їх інтеграції в аналітичний процес.

**Мета роботи:** розробити й апробувати комплексну методику застосування інструментів ШІ в OSINT-дослідженнях.

**Наукова новизна дослідження** полягає в розробці методики інтеграції ШІ в OSINT-цикл, класифікації інструментів та прототипу ШІ-асистента.

**Практичне значення дослідження** полягає в застосуванні цих рішень аналітичними підрозділами, фахівцями з безпеки, журналістами-розслідувачами та OSINT-спільнотами для підвищення ефективності аналізу відкритих даних.

**Методи дослідження:** аналіз наукових джерел, порівняльний аналіз ШІ- інструментів, комп'ютерний експеримент з тестуванням прототипу, моделювання архітектури OSINT-системи.

**Наукова новизна дослідження** полягає в розробці методики інтеграції ШІ в OSINT-цикл, класифікації ШІ-інструментів, моделі вибору інструментарію та прототипу ШІ-асистента.

**Ключові слова:** розвідка з відкритих джерел (OSINT), штучний інтелект, машинне навчання, NLP, комп'ютерний зір, OSINT-цикл, верифікація даних, дезінформація, deepfake, геолокація, ШІ-асистент.

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

**OSINT** – розвідка з відкритих джерел (Open Source Intelligence)

**ШІ** – штучний інтелект (Artificial Intelligence)

**ML** – машинне навчання (Machine Learning)

**DL** – глибоке навчання (Deep Learning)

**NLP** – обробка природної мови (Natural Language Processing)

**CV** – комп'ютерний зір (Computer Vision)

**LLM** – великі мовні моделі (Large Language Model)

**GAN** – генеративні змагальні мережі (Generative Adversarial Networks)

**GDPR** – Загальний регламент захисту даних Європейського Союзу (General Data Protection Regulation)

**ШІ Act** – Регламент ЄС про штучний інтелект (Artificial Intelligence Act)

**NATO** – Організація Північноатлантичного договору (North Atlantic Treaty Organization)

**ЄС (EU)** – Європейський Союз (European Union)

**FBI** – Федеральне бюро розслідувань США (Federal Bureau of Investigation)

**API** – прикладний програмний інтерфейс (Application Programming Interface)

**URL** – уніфікований покажчик ресурсу (Uniform Resource Locator)

**GPT-4** – Generative Pre-trained Transformer 4, велика мовна модель для роботи з текстами

**BERT** – Bidirectional Encoder Representations from Transformers, мовна модель для NLP

**YOLO** – You Only Look Once, архітектура для детекції об'єктів на зображеннях і відео

**SpaCy** – програмна бібліотека для обробки природної мови (NLP)

**OVIS** – модель комп'ютерного зору для розпізнавання об'єктів на зображеннях

**Sensity** – платформа ШІ для виявлення deepfake-контенту

**Reality Defender** – сервіс на основі ШІ для детекції маніпульованого мультимедійного контенту

**deepfake** – штучно згенерований або змінений аудіовізуальний контент з імітацією зовнішності чи голосу реальних осіб

# ВСТУП

Сучасний розвиток інформаційних технологій та штучного інтелекту (ШІ) докорінно змінює підходи до аналізу відкритих даних у розвідувальній діяльності. OSINT (розвідка з відкритих джерел) стрімко утвердився як ключовий метод отримання розвідувальної інформації з публічно доступних джерел - соціальних мереж, новинних сайтів, баз даних тощо. Інтеграція технологій ШІ в процеси OSINT є новітнім напрямом, що відкриває можливості для автоматизації збору та обробки величезних обсягів інформації, підвищення оперативності аналізу та точності отриманих результатів [1, 2]. ШІ вже зараз розглядається як революційний інструмент у сфері OSINT: він здатен прискорювати проведення розслідувань за рахунок виконання рутинних завдань, машинного аналізу даних і виявлення прихованих закономірностей, недоступних для ручного опрацювання. Таким чином, поєднання OSINT та ШІ формує актуальний науково - практичний напрям, що відповідає викликам сучасності.

В умовах інформаційної перенасиченості, зростання ролі соціальних медіа, гібридних загроз і кібератак обсяги відкритих даних зростають експоненційно. Щодня створюються терабайти нових зображень, відео, повідомлень, реєстрів та супутникових знімків. Такий масштаб даних робить традиційні (людинозалежні) методи OSINT малоефективними або повністю непридатними. Саме тут відкривається потенціал штучного інтелекту (ШІ).

ШІ - це галузь, що охоплює моделі машинного навчання (ML), глибинного навчання (DL), обробки природної мови (NLP), комп'ютерного зору (CV), які дозволяють автоматизувати аналіз складних і неструктурованих даних [5, 6]. У контексті OSINT ШІ відкриває нові можливості: від автоматичного моніторингу соціальних мереж до геолокації зображень, від розпізнавання об'єктів на відео до виявлення дезінформації в інформаційних кампаніях.

**Актуальність теми.** Обрана тема дослідження обумовлена зростаючою роллю OSINT у різних сферах - від національної безпеки та кібербезпеки до журналістики й бізнес - розвідки - де критично важливим є своєчасне отримання достовірної інформації. В цифрову епоху обсяги відкритих даних збільшуються експоненційно: соціальні мережі, онлайн - медіа та відкриті реєстри щоденно генерують величезні масиви інформації. Обробка цих даних традиційними методами є трудомісткою і потребує значних людських ресурсів, через що зростає ризик пропустити важливі деталі або тенденції. Актуальність впровадження ШІ в OSINT зумовлена необхідністю підвищити ефективність і швидкість аналізу: алгоритми машинного навчання здатні автоматично фільтрувати інформаційний шум, виявляти релевантні повідомлення та агрегувати дані з численних джерел у стислий, зручний для аналізу формат. Це дозволяє аналітикам зосередитися на інтерпретації отриманих відомостей замість рутинного збору, що особливо важливо при моніторингу кризових чи надзвичайних ситуацій.

Актуальність дослідження підсилюється й сучасними викликами у сфері інформаційної безпеки та гібридних загроз. Поширення дезінформації, маніпулятивного контенту і навіть використання генеративних технологій (наприклад, дипфейків) вимагає нових підходів до перевірки та верифікації відкритих даних. Застосування ШІ в OSINT відкриває шлях до автоматизованого виявлення аномалій та підозрілих елементів у великих масивах мультимедійної інформації. Показовим є досвід розслідування подій російсько - української війни, коли фахівці OSINT оперативно використовували дописи в соцмережах і супутникові знімки для перевірки повідомлень про бойові дії та руйнування. Алгоритми штучного інтелекту здатні значно підсилити такі зусилля: вони автоматично аналізують відео - та фотоматеріали, виділяючи ключові деталі і ідентифікуючи об’єкти чи осіб, що суттєво економить час і підвищує надійність отриманої інформації. Отже, впровадження ШІ в процеси OSINT є на часі та відповідає нагальній потребі

протидіяти інформаційним загрозам і швидко отримувати знання з відкритих джерел.

**Наукова новизна** одержаних результатів полягає в розробці та обґрунтуванні комплексної методики застосування сучасних алгоритмів штучного інтелекту для автоматизації OSINT - досліджень. На відміну від відомих підходів, у роботі запропоновано інтеграцію методів машинного навчання (обробки природної мови, комп'ютерного зору, прогнозної аналітики тощо) безпосередньо в цикл OSINT - розвідки, що дозволяє якісно новий рівень опрацювання відкритих даних.

Запропонована методика розширює теоретичні засади OSINT, поєднуючи класичні принципи розвідки з відкритих джерел із можливостями штучного інтелекту щодо виявлення прихованих зв'язків та трендів у великих масивах інформації. Практична значущість роботи полягає у тому, що результати дослідження можуть бути безпосередньо впроваджені в діяльність аналітичних підрозділів та інших фахівців, які займаються OSINT. Розроблена методика та рекомендації дозволять суттєво підвищити оперативність і точність збору та аналізу даних з відкритих джерел, що сприятиме більш ефективному виявленню загроз, розслідуванню інцидентів та прийняттю обґрунтованих рішень у сферах безпеки, журналістських розслідувань тощо.

**Об'єктом дослідження** є процеси збору, обробки та інтерпретації відкритої інформації за допомогою інструментів OSINT.

**Предмет дослідження:** методи, моделі та інструменти штучного інтелекту для підвищення ефективності OSINT - досліджень, а також принципи їх інтеграції в аналітичний процес.

**Мета і завдання дослідження.** Метою даного дослідження є підвищення ефективності процесів OSINT - розвідки шляхом розробки та впровадження методів штучного інтелекту для автоматизації збору й аналізу інформації з відкритих джерел.

Відповідно до поставленої мети в роботі необхідно вирішити такі **завдання:**

1. Проаналізувати теоретичні основи та сучасний стан розвитку OSINT, уточнити понятійний апарат і визначити ключові проблеми, що виникають при опрацюванні даних з відкритих джерел.

2. Дослідити можливості, існуючі підходи і програмні інструменти застосування штучного інтелекту в сфері OSINT; виявити переваги та обмеження наявних рішень.

3. Розробити концепцію та методику практичного використання алгоритмів ШІ (зокрема методів машинного навчання) для автоматизації рутинних завдань OSINT і підвищення якості аналізу розвідувальної інформації.

4. Реалізувати програмний прототип системи OSINT з елементами штучного інтелекту та провести експериментальну перевірку запропонованих рішень на прикладі тестових сценаріїв або реальних кейсів з відкритих джерел.

5. Оцінити ефективність розробленої методики (за критеріями швидкості обробки даних, повноти та точності виявленої інформації тощо) та сформулювати рекомендації щодо її практичного застосування й подальшого удосконалення.

**Методи дослідження.** Для розв’язання визначених завдань застосовано комплекс методів дослідження: теоретичних - аналіз і синтез наукової літератури, нормативних документів і публікацій з питань OSINT та ШІ, порівняльний аналіз існуючих технологій; емпіричних - збір даних з відкритих онлайн - джерел, спостереження за роботою наявних OSINT - інструментів, експертне оцінювання результатів роботи алгоритмів; експериментальних - проведення комп’ютерного експерименту з тестування розробленого прототипу на спеціально сформованих наборах даних, вимірювання показників ефективності та точності; методів проєктування та моделювання - побудова архітектури програмної системи OSINT з використанням ШІ, моделювання процесів збору й аналізу інформації, розробка і тренування моделей машинного навчання для вирішення прикладних завдань розвідки з відкритих джерел.

**Структура роботи.** Магістерська робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. У першому розділі викладено теоретичні засади розвідки з відкритих джерел та проаналізовано можливості застосування технологій штучного інтелекту в OSINT - дослідженнях. Другий розділ присвячено аналізу сучасних методів і програмних засобів штучного інтелекту, що використовуються для автоматизації OSINT, а також розробці власної методики інтеграції ШІ в процес збору та аналізу відкритих даних. У третьому розділі представлено практичну реалізацію запропонованої методики у вигляді програмного прототипу, описано проведення експериментальних досліджень на прикладах типових OSINT - сценаріїв та наведено оцінку ефективності розробленого рішення. У **висновках** узагальнено результати роботи, сформульовано підсумкові висновки щодо досягнення мети та виконання завдань дослідження, а також рекомендації щодо впровадження отриманих результатів.

**Ключові слова:** розвідка з відкритих джерел (OSINT); ШІ; машинне навчання; обробка природної мови; комп’ютерний зір; автоматизація OSINT; аналіз даних.

# РОЗДІЛ 1
# АНАЛІЗ СУЧАСНОГО СТАНУ ПРОБЛЕМИ ІНТЕГРАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ В OSINT - ДОСЛІДЖЕННЯ

## 1.1 Теоретичні засади та еволюція OSINT як науково - практичної дисципліни

Розвідка з відкритих джерел (Open Source Intelligence, OSINT) - це міждисциплінарна сфера, що поєднує елементи інформатики, аналітики, соціології, журналістики та права. Її головною відмінністю від інших форм розвідки є використання виключно легально доступної інформації без порушення норм законодавства. Згідно з визначенням НАТО, OSINT розглядається як інтелектуальний продукт, що створюється на основі збору, обробки та інтерпретації даних з відкритих джерел [6].

Джерела OSINT охоплюють широкий спектр інформаційних ресурсів: офіційні урядові документи, бази даних і реєстри, статистичні звіти, матеріали ЗМІ, соціальні мережі, геопросторові дані, супутникові знімки, краудсорсингові платформи, фото - та відеоконтент [1; 7]. Основна мета такої розвідки полягає в отриманні достовірної, верифікованої та релевантної інформації, що може бути використана в безпековій, економічній, правозахисній, журналістській та корпоративній діяльності [8].

У міжнародній практиці OSINT розглядається як інструмент «м'якої сили», що забезпечує прозорість, верифікацію та доказовість у різних сферах. Його активно застосовують у кримінальній розвідці (law enforcement intelligence), військовій сфері, корпоративній безпеці, інформаційних операціях і цифровій журналістиці. Відомі організації на кшталт Bellingcat, Centre for Information Resilience та Amnesty International широко використовують OSINT для верифікації воєнних злочинів, документування порушень прав людини та моніторингу переміщення військової техніки [2; 3].

Еволюція розвитку OSINT - технологій має поступовий характер і відображає загальні тенденції цифрової трансформації суспільства. Від традиційних методів збору публічної інформації до комплексних аналітичних систем, інтегрованих зі штучним інтелектом, спостерігається якісний перехід від ручного аналізу до автоматизованої обробки великих даних. Умовно розвиток OSINT можна поділити на три ключові етапи, що наведено в таблиці 1.1.

Таблиця 1.1 - Етапи еволюції OSINT - технологій

| Етап | Хронологічні межі | Характеристика етапу |
|---|---|---|
| Перший етап - класичний (до 2000 - х років) | До 2000 р. | Формування концепції розвідки з відкритих джерел як допоміжного аналітичного інструменту. Аналіз текстових публікацій, документів, архівів і традиційних ЗМІ. Обробка інформації переважно вручну. |
| Другий етап - цифровий (2000 - 2015 рр.) | 2000 - 2015 | Перехід до цифрового середовища, поява інструментів автоматизованого збору даних. Активне використання інтернету, пошукових систем, онлайн - форумів та соціальних мереж. Застосування веб - скрейпінгу та супутникових знімків. |
| Третій етап - інтелектуальний (з 2015 року і дотепер) | 2015 - сьогодення | Інтеграція технологій штучного інтелекту, машинного навчання, комп’ютерного зору та геоаналітики. Автоматизація збору, аналізу та верифікації даних. Використання генеративних моделей і мультиагентних систем. |

Аналіз етапів розвитку OSINT, згруповані та продемонстровані у табл. 1.1 дає підстави стверджувати, що сучасна розвідка з відкритих джерел пройшла шлях від традиційних форм журналістсько - аналітичного збору інформації до високотехнологічної системи, заснованої на штучному інтелекті та автоматизації процесів. Зміна парадигми від «ручного аналізу» до «аналітики на основі ШІ» суттєво підвищила швидкість обробки даних, точність виявлення закономірностей і рівень достовірності отриманих результатів. Таким чином, OSINT сьогодні є не лише допоміжним, а стратегічним інструментом інформаційної безпеки та розвідки в умовах цифрової епохи.

Важливо підкреслити, що кожен етап розвитку OSINT супроводжувався появою організацій та ініціатив, які демонстрували практичну цінність цієї дисципліни. Наприклад, відомі журналістські розслідувальні проекти Bellingcat та Conflict Intelligence Team (CIT) широко використовують OSINT для аналізу супутникових знімків, геолокації фотографій та ідентифікації військової техніки [10].

У журналістиці яскравими прикладами є проекти NYT Visual Investigations та BBC Verify, які застосовують OSINT для перевірки фактів і відстеження поширення дезінформації [11].

Особливої уваги заслуговує досвід України, де OSINT став одним із ключових інструментів документування воєнних злочинів та відстеження переміщень військової техніки РФ під час повномасштабної агресії [12]. Платформи на кшталт InformNapalm та Molfar поєднують аналітичну роботу волонтерів з використанням інструментів штучного інтелекту для збору і верифікації даних.

У правоохоронній практиці США та ЄС OSINT розглядається як критично важливий компонент кримінальної розвідки. Зокрема, за даними Федерального бюро розслідувань (FBI), понад 70% відкритих джерел, що аналізуються аналітиками, мають прикладне значення для розслідувань у сфері кіберзлочинності [13].

Джорджтаун, понад 80% інформації, що використовується в стратегічній аналітиці США, надходить з відкритих джерел, що підтверджує значущість OSINT у сучасній системі безпеки [5].

Разом із розвитком цифрових технологій зростають і виклики для OSINT. Серед основних викликів, з якими стикаються дослідники у сфері OSINT, варто виділити надмірність доступних даних, що потребують ретельної фільтрації та структурування; високий рівень дезінформації й поширення маніпулятивних повідомлень, які ускладнюють формування об’єктивної аналітичної картини; складність верифікації мультимедійного контенту, особливо в умовах зростання кількості штучно згенерованих

матеріалів; необхідність оперативного реагування на події в кризових ситуаціях, коли швидкість обробки інформації є критичною; а також наявність юридичних та етичних обмежень, пов’язаних із використанням персональних даних та дотриманням принципів інформаційної безпеки [10].

Таким чином, OSINT поступово трансформувався з допоміжного інструменту розвідки НАТО у самостійну науково - практичну дисципліну, яка формує нову культуру інформаційного мислення, засновану на відкритості, доказовості та незалежності. У контексті гібридних війн, кібератак і маніпулятивних кампаній OSINT стає одним із ключових інструментів цифрового опору та глобальної безпеки.

## 1.2 Роль та місце штучного інтелекту в трансформації методів розвідки з відкритих джерел

В першу чергу, варто охарактеризувати та розкрити сутність штучного інтелекту. ШІ визначається як здатність технічних систем обробляти та інтерпретувати зовнішні дані, навчатися на їхній основі та використовувати отримані знання для досягнення конкретних цілей шляхом гнучкої адаптації до умов навколишнього середовища. Водночас, інтелектуальні системи мають на меті забезпечувати прийняття якісних, обґрунтованих та ефективних рішень у складних умовах, коли традиційні методи аналізу не можуть забезпечити належної точності або ефективності.

Спрощено, ШІ можна визначити як систему, що не тільки виконує задані дії, але й навчається на основі досвіду, розпізнає закономірності та приймає рішення, спираючись на вхідні дані. Ці властивості забезпечують ШІ можливість постійного самовдосконалення, що робить його ефективним інструментом у різних галузях, зокрема в освіті. Зокрема, алгоритми машинного навчання, що є невід’ємною складовою сучасних ШІ - систем, можуть розв’язувати широкий спектр завдань, зокрема оптимізацію рішень у сферах природоохоронної діяльності, соціальної справедливості, а також

створення інструментів для вирішення глобальних викликів. Наприклад, вони дозволяють визначати найоптимальніші території для природоохоронних мереж з урахуванням складної сукупності екологічних параметрів. Водночас, машинне навчання може підвищити об’єктивність і справедливість рішень, що має особливе значення в контексті соціальної відповідальності сучасних технологій.

Окрім машинного навчання ШІ має інші складові, які працюють у системі при цьому поєднуючи великі обсяги даних з інтелектуальними ітеративними алгоритмами обробки. У свою чергу, поєднання складових дозволяють штучному інтелекту навчатися на основі шаблонів та особливостей проведеного аналізу даних. Кожен раз, коли система здійснює цикл обробки інформації, вона оцінює та аналізує свою ефективність, застосовуючи отримані дані для подальшого вдосконалення й набуття нових навичок.

Важливими складовими ШІ, без яких він не може існувати є машинне навчання (Machine learning, ML), яке вже було згадано раніше, та глибоке навчання, мається на увазі підкатегорія машинного, яка дозволяє імітувати нейронну мережу людського мозку. Власне глибоке навчання дозволяє розпізнавати закономірності, шуми та джерела плутанини в даних. Нейронні мережі, що використовуються в рамках глибокого навчання (Deep Learning), стають можливими завдяки штучним нейронним мережам, які імітують роботу нейронів або клітин мозку. Ці моделі застосовують принципи математики та комп’ютерних наук для відтворення процесів мислення, що забезпечує більш універсальний процес навчання.

Нейронні мережі складаються з трьох шарів: вхідного, прихованого та вихідного, і можуть містити тисячі або навіть мільйони вузлів. Інформація надходить через вхідний шар, де вхідні дані отримують певну вагу. З’єднані між собою вузли множать вагу зв’язків під час передачі даних. Для того щоб навчатися на власному досвіді, система порівнює результати обчислень мережі з очікуваними результатами і коригує зв’язки, ваги та пороги на основі

виявлених розбіжностей. На рис. 1.1 зображені ключові складові штучного інтелекту.


Рисунок. 1.1 - Ключові складові штучного інтелекту

На рис. 1.1 ми бачимо, що штучний інтелект формується як комплексна система, у центрі якої лежать глибинне навчання та нейронні мережі. Саме ці технології забезпечують здатність ШІ аналізувати великі масиви даних, розпізнавати складні патерни та приймати наближені до людських рішення.

Важливо зазначити, що ключова мета штучного інтелекту полягає не лише в тому, щоб забезпечити точність або об’єктивність прийнятих рішень, але і в подальшій їхній ефективній реалізації. Окрім того, сучасні технології ШІ мають потенціал для створення нових інструментів та рішень, які можуть зробити істотний внесок у розв’язання нагальних світових проблем, включно з соціальними, екологічними та економічними викликами.

Упродовж останнього десятиліття ШІ став ключовим чинником трансформації розвідки з відкритих джерел (OSINT). Якщо на початкових етапах розвиток OSINT ґрунтувався переважно на ручному зборі та верифікації інформації, то сучасні тенденції демонструють перехід до масштабованих автоматизованих рішень. Це зумовлено як зростанням обсягів даних у відкритому доступі (соціальні мережі, відеохостинги, відкриті бази даних), так і необхідністю оперативного аналізу інформації для прийняття рішень у режимі реального часу.

У науковій літературі ШІ визначається як здатність комп'ютерних систем виконувати функції, що традиційно асоціюються з людським інтелектом - навчання, міркування, планування, розпізнавання мовлення та образів [11]. У контексті OSINT це означає автоматизацію таких процесів, як пошук релевантних даних, класифікація джерел, виявлення аномалій, перевірка достовірності контенту.

Основні напрями інтеграції технологій штучного інтелекту в OSINT - сферу наведено у таблиці 1.2. Вони охоплюють ключові галузі сучасного ШІ - від машинного навчання до генеративних моделей, які істотно впливають на точність, швидкість і достовірність аналітичних процесів.

Таблиця 1.2 - Основні напрями інтеграції технологій штучного інтелекту в OSINT - дослідження

| Напрям інтеграції | Коротка характеристика | Типові приклади застосування |
|---|---|---|
| Машинне навчання (Machine Learning, ML) | Використовується для виявлення закономірностей і кореляцій у великих масивах даних. Алгоритми класифікації та кластеризації дозволяють групувати інформацію, виявляти приховані зв'язки та аномалії. | Відстеження переміщень військової техніки за супутниковими знімками; аналіз поведінкових шаблонів користувачів у соцмережах; прогнозування інформаційних потоків. |
| Обробка природної мови (Natural Language Processing, NLP) | Забезпечує автоматизований аналіз текстових даних - від пошуку ключових слів до глибинного семантичного розуміння змісту повідомлень. Використовується для виявлення дезінформації та пропагандистських наративів. | Аналіз тональності постів, виявлення координаційних кампаній, побудова семантичних карт інформаційних потоків (BERT, GPT - 4, SpaCy). |
| Комп'ютерний зір (Computer Vision, CV) | Орієнтований на автоматичну обробку візуальних даних (зображень, відео, супутникових знімків). Дозволяє ідентифікувати об'єкти, визначати геолокацію, аналізувати зміни у просторі. | Розпізнавання номерних знаків, ідентифікація військової техніки, аналіз відеоспостереження, геолокація за візуальними орієнтирами (YOLO, ResNet, OVIS). |
| Генеративні моделі (Generative Adversarial Networks, GAN) | Використовуються для створення синтетичних даних (зображень, відео, аудіо), що становить виклик для OSINT - аналітики. Потребують розвитку систем верифікації для виявлення фейкових матеріалів. | Виявлення deepfake - контенту, розробка алгоритмів детекції підроблених фото і відео (Sensity ШІ, Reality Defender). |

Проведений аналіз дає змогу дійти висновку, що інтеграція технологій штучного інтелекту в OSINT - дослідження забезпечує суттєве підвищення ефективності збору, аналізу та верифікації інформації. Використання ML, NLP і CV - технологій сприяє автоматизації рутинних процесів та розширює аналітичні можливості, тоді як поява генеративних моделей висуває нові виклики у сфері перевірки достовірності даних, формуючи потребу в розвитку контр - технологій детекції фальсифікацій.

Окремої уваги потребує вплив великих мовних моделей (LLM) на процес OSINT - досліджень. Сучасні моделі, такі як GPT - 4, Claude, Gemini, дозволяють автоматизувати семантичний пошук, здійснювати переклад та резюмування великих обсягів даних, виявляти повторювані наративи та аномалії [27]. Водночас їх застосування ускладнюється ризиком «галюцинацій» (створення неправдивих фактів), що потребує обов’язкової верифікації отриманих результатів.

Порівняння ручних і ШІ - орієнтованих методів аналізу показує, що використання ШІ дозволяє зменшити час опрацювання великих масивів текстових даних у середньому на 40 - 60%, водночас забезпечуючи вищий рівень точності класифікації повідомлень [28].

Інтеграція ШІ в OSINT змінює саму природу цієї дисципліни. Якщо раніше головним обмеженням був людський ресурс, то сьогодні основною перевагою стає здатність ШІ швидко обробляти великі обсяги даних, зменшуючи ризики помилок і упередженості. Це не лише підвищує точність оцінок, а й відкриває нові можливості для прогнозування та виявлення загроз.

## 1.3 Критичний аналіз існуючих методологій та моделей застосування ШІ в OSINT

У сучасних дослідженнях представлено низку підходів до інтеграції штучного інтелекту в OSINT - процеси. Вони охоплюють як окремі технічні рішення (наприклад, автоматизований парсинг даних, класифікація зображень, аналіз тональності текстів), так і спроби побудови методологічних рамок. Однак більшість запропонованих моделей характеризуються обмеженою сферою застосування та не враховують повного життєвого циклу OSINT - дослідження [15].

Зокрема, дослідники відзначають, що переважна частина наявних підходів зосереджена на окремих етапах, таких як збір даних або автоматизований аналіз, тоді як питання верифікації, пояснюваності результатів чи візуалізації залишаються поза увагою. У практиці відомих організацій (Bellingcat, EU Disinfo Lab) також відсутні універсальні стандартизовані протоколи інтеграції ШІ - здебільшого застосовуються “точкові” інструменти, залежно від конкретного кейсу. Також існуюча модель має певні недоліки, наведено на рис. 1.1.

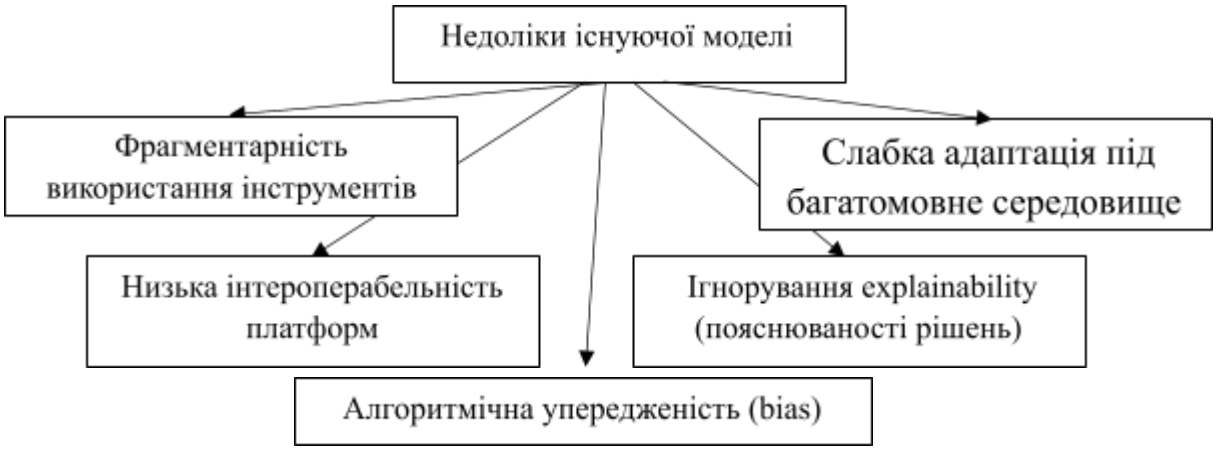


Рисунок 1.2 - Недоліки існуючої моделі

На рис. 1.2 можна побачити, що недоліки чинної моделі застосування ШІ - інструментів у OSINT пов’язані не лише з технічними обмеженнями, а й

із системною несумісністю платформ та відсутністю прозорості алгоритмів. Фрагментарність використання інструментів, слабка адаптація до багатомовного середовища та ризики алгоритмічної упередженості свідчать про необхідність комплексного підходу до інтеграції ШІ у розслідувальні процеси.

Розглянемо кожен із виявлених недоліків більш детально. Перший недолік є фундаментальним і полягає у фрагментарності використання інструментів. Багато сучасних рішень охоплюють лише окремі етапи OSINT - ланцюга - збір, аналіз або перевірку даних, - що створює розриви між ними та знижує узгодженість результатів. Відсутність комплексного підходу призводить до дублювання операцій і втрати частини важливої інформації.

Другий недолік стосується низької інтероперабельності платформ. Більшість інструментів не мають уніфікованих форматів даних або спільних інтерфейсів, через що результати, отримані в одній системі, складно інтегрувати в іншу без ручної або додаткової обробки. Це ускладнює побудову наскрізних аналітичних процесів і знижує швидкість роботи аналітика.

Третій недолік пов’язаний з ігноруванням принципу пояснюваності (explШInability). Значна частина моделей не забезпечує прозорості власних алгоритмів, що унеможливлює перевірку джерел і логіки прийнятих рішень. Це підвищує ризик маніпуляцій і знижує рівень довіри до результатів ШІ - аналізу, особливо у випадках, коли від цих результатів залежать практичні рішення.

Четвертий недолік полягає у слабкій адаптації моделей до багатомовного середовища. Переважна більшість NLP - рішень оптимізована під англомовні корпуси даних, тоді як ефективність їхньої роботи з українською, російською чи іншими мовами суттєво нижча. Це обмежує можливості дослідників у контексті аналізу регіональних інформаційних просторів і знижує точність висновків при багатомовному моніторингу.

Отже, усунення зазначених недоліків є ключовою передумовою для формування комплексної, прозорої та адаптивної моделі застосування штучного інтелекту в OSINT - дослідженнях.

Окрім технічних недоліків, варто відзначити “білі плями” в оцінюванні ефективності. Більшість досліджень не пропонують чітких метрик для порівняння результатів ШІ - моделей із традиційними методами OSINT - аналізу. Також обмеженою залишається кількість апробацій на реальних кейсах воєнного чи кризового характеру, де якість і швидкість аналізу мають критичне значення [16].

Серед відомих прикладних рішень варто згадати IBM i2 Analyst’s Notebook та Palantir Gotham, які поєднують інструменти аналізу даних із візуалізацією взаємозв’язків, проте їх інтеграція з ШІ - модулями обмежена та закрита для широкого кола користувачів [29]. Натомість open - source платформи, такі як Maltego або Gephi, дозволяють створювати графи зв’язків, проте вимагають ручного налаштування та не підтримують автоматизовану верифікацію даних.

Відсутність єдиних стандартів інтеграції ШІ в OSINT підтверджує і NATO OSINT Handbook (2020), де зазначається, що використання алгоритмів залежить від окремого кейсу та доступності даних, без формалізованої універсальної методики [6].

Таким чином, існуючі методології та моделі інтеграції ШІ в OSINT не забезпечують комплексного підходу. Це створює передумови для розробки нової, цілісної методики, яка врахує всі етапи життєвого циклу OSINT - дослідження, забезпечить інтероперабельність інструментів та адаптованість до багатомовного середовища.

## 1.4 Огляд правових та етичних фреймворків, що регулюють використання ШІ та обробку даних (GDPR, ШІ Act тощо)

Використання штучного інтелекту у сфері OSINT відбувається в умовах складного правового та етичного контексту. На відміну від традиційних методів аналізу даних, застосування алгоритмів ШІ часто супроводжується ризиками порушення приватності, дискримінації та непрозорості прийняття рішень. Тому міжнародна спільнота розробила низку регуляторних актів і рекомендацій, які визначають принципи та обмеження у використанні інтелектуальних систем.

Основні напрями інтеграції технологій штучного інтелекту в OSINT - сферу наведено у таблиці 1.2. Вони охоплюють ключові галузі сучасного ШІ - від машинного навчання до генеративних моделей, які істотно впливають на точність, швидкість і достовірність аналітичних процесів.

Таблиця 1.2 - Основні напрями інтеграції технологій штучного інтелекту в OSINT - дослідження

| Напрям інтеграції | Коротка характеристика | Типові приклади застосування |
|---|---|---|
| Машинне навчання (Machine Learning, ML) | Використовується для виявлення закономірностей і кореляцій у великих масивах даних. Алгоритми класифікації та кластеризації дозволяють групувати інформацію, виявляти приховані зв’язки та аномалії. | Відстеження переміщень військової техніки за супутниковими знімками; аналіз поведінкових шаблонів користувачів у соцмережах; прогнозування інформаційних потоків. |
| Обробка природної мови (Natural Language Processing, NLP) | Забезпечує автоматизований аналіз текстових даних - від пошуку ключових слів до глибинного семантичного розуміння змісту повідомлень. Використовується для виявлення дезінформації та пропагандистських наративів. | Аналіз тональності постів, виявлення координаційних кампаній, побудова семантичних карт інформаційних потоків (BERT, GPT - 4, SpaCy). |
| Комп’ютерний зір (Computer Vision, CV) | Орієнтований на автоматичну обробку візуальних даних (зображень, відео, супутникових знімків). Дозволяє ідентифікувати об’єкти, визначати геолокацію, аналізувати зміни у просторі. | Розпізнавання номерних знаків, ідентифікація військової техніки, аналіз відеоспостереження, геолокація за візуальними орієнтирами (YOLO, ResNet, OVIS). |

| | | |
|---|---|---|
| Генеративні моделі (Generative Adversarial Networks, GAN) | Використовуються для створення синтетичних даних (зображень, відео, аудіо), що становить виклик для OSINT - аналітики. Потребують розвитку систем верифікації для виявлення фейкових матеріалів. | Виявлення deepfake - контенту, розробка алгоритмів детекції підроблених фото і відео (Sensity ШІ, Reality Defender). |

Проведений аналіз та наведені результати у табл. 1.2 дають змогу дійти до висновку, що інтеграція технологій штучного інтелекту в OSINT - дослідження забезпечує суттєве підвищення ефективності збору, аналізу та верифікації інформації. Використання ML, NLP і CV - технологій сприяє автоматизації рутинних процесів та розширює аналітичні можливості, тоді як поява генеративних моделей висуває нові виклики у сфері перевірки достовірності даних, формуючи потребу в розвитку контр - технологій детекції фальсифікацій.

Паралельно з правовим регулюванням сформувалася система етичних принципів, що покликана забезпечити відповідальне використання ШІ. Найбільш поширеними вважаються такі [21]:

- мінімізація шкоди (avoid harm) - ШІ не повинен завдавати непропорційних ризиків суспільству чи окремим особам;

- прозорість і пояснюваність (transparency & explШInability) - користувач має право розуміти логіку роботи системи;

- захист приватності (privacy protection) - особисті дані повинні оброблятися з дотриманням принципів GDPR;

- справедливість і недискримінація (fШIrness & non - discrimination) - алгоритми не повинні відтворювати або посилювати соціальні упередження.

Європейський ШІ Act класифікує системи штучного інтелекту за чотирма рівнями ризику:

- неприйнятний ризик (заборонені системи, як - от біометричний моніторинг у публічних просторах у режимі реального часу);

- високий ризик (системи, що використовуються у сфері критичної інфраструктури, освіти, працевлаштування, правоохоронної діяльності);

- обмежений ризик (системи, що потребують прозорості для користувача, наприклад чат - боти);

- мінімальний ризик (усі інші системи).

У сфері OSINT найбільший інтерес становить категорія високоризикових систем, які потребують суворої сертифікації та пояснюваності результатів [30].

Окрім ЄС, етичні рекомендації публікували також IEEE (Ethically Aligned Design) та UNESCO (Recommendation on the Ethics of Artificial Intelligence, 2021). У цих документах наголошується на принципах «algorithmic accountability» (підзвітності алгоритмів) та «human oversight» (необхідності людського контролю над критичними рішеннями) [31].

Для сфери OSINT правові та етичні дилеми мають особливу актуальність. Аналітики часто працюють із великими масивами даних, що включають персональну інформацію користувачів соціальних мереж, фото - та відеоматеріали, геолокаційні дані. Це створює ризик порушення балансу між публічним інтересом (наприклад, документування воєнних злочинів) і правом на приватність.

Додаткові загрози виникають у зв’язку з поширенням генеративних моделей ШІ, які можуть використовуватися для створення фейкового контенту (deepfake), маніпуляцій громадською думкою або несанкціонованого вилучення даних. Саме тому міжнародні організації наголошують на необхідності чіткого дотримання принципів етичного використання та правових обмежень у діяльності OSINT - аналітиків [22].

***Висновки до розділу 1***

Аналіз теоретичних засад, еволюції OSINT та ролі штучного інтелекту у розвідці з відкритих джерел показує, що ця дисципліна пройшла значну трансформацію: від аналітики текстових документів до комплексних цифрових досліджень із використанням мультимедійних даних, супутникових

знімків та інструментів автоматизації. Сучасний OSINT поєднує методи збору, обробки, аналізу та синтезу інформації з відкритих джерел і застосовується у кримінальній, військовій, корпоративній та журналістській сферах.

Інтеграція штучного інтелекту суттєво змінила підходи до аналізу даних, дозволяючи автоматизувати процеси обробки великих обсягів інформації, підвищити точність аналітичних оцінок та зменшити вплив людського фактору. Основні технології, що застосовуються в OSINT, включають машинне навчання, обробку природної мови, комп'ютерний зір та генеративні моделі, що відкривають нові можливості для швидкого та точного аналізу даних.

Разом із цим, критичний аналіз існуючих методологій показав, що більшість підходів є фрагментарними, не охоплюють повний життєвий цикл OSINT, мають низьку інтероперабельність і слабко адаптовані до багатомовного середовища. Також часто ігноруються пояснюваність рішень і ризики алгоритмічної упередженості, а оцінка ефективності інструментів обмежується вузьким колом кейсів. Це свідчить про потребу у розробці комплексної методики, яка об'єднає всі етапи процесу та адаптує ШІ - інструменти до практичних завдань.

Окрему увагу слід приділяти правовим та етичним аспектам. Регламенти GDPR та ШІ Act, а також міжнародні етичні принципи визначають межі допустимого використання ШІ і персональних даних, наголошуючи на прозорості, мінімізації шкоди, справедливості та захисті приватності. У контексті OSINT це означає баланс між публічним інтересом та правом на приватність, особливо при роботі з мультимедійними даними, генеративними моделями та верифікацією інформації.

Таким чином, потенціал штучного інтелекту в OSINT є величезним, проте ефективне його застосування потребує комплексного підходу, що враховує технологічні, методологічні, правові та етичні аспекти. Подальші дослідження мають бути спрямовані на формалізацію методології, адаптацію

моделей до практичних потреб та оцінку ефективності інструментів у різних контекстах - від безпеки та журналістики до кризового управління.

Метою цієї роботи є створення комплексної методики практичного використання сучасних інструментів штучного інтелекту для OSINT - досліджень з урахуванням технічних, правових та етичних обмежень.

# РОЗДІЛ 2
# РОЗРОБКА КОМПЛЕКСНОЇ МЕТОДИКИ ЗАСТОСУВАННЯ ШІ В OSINT - ДОСЛІДЖЕННЯХ

## 2.1 Розробка критеріїв та проведення класифікації сучасних ШІ - інструментів для OSINT

Для ефективного застосування ШІ в OSINT важливо не лише знати наявні інструменти, а й системно їх класифікувати за функціональними та технічними характеристиками. Класифікація дозволяє аналітикам швидко визначати, які інструменти підходять для конкретних завдань, оптимізувати процес збору і обробки даних та підвищити точність аналітичних висновків.

В першу чергу, критерії для проведення класифікації сучасних ШІ - інструментів що застосовуються в OSINT дослідженнях, повинні базуватися на принципах відповідності функціональним етапам аналітичного процесу OSINT. Даний підхід дозволяє логічно пов'язати і розподілити типи інструментів із певним етапом розвідувального циклу, що має на меті підвищити системність та точність подальшого аналітичного алгоритму. Варто охарактеризувати кожен принцип більш детально.

1.Принцип збору та попередньої фільтрації даних визначає початковий етап OSINT - аналізу, що полягає у виявленні, зборі та структуризації інформації з відкритих джерел. На цьому етапі формується первинна база даних, від точності та повноти якої залежить достовірність подальших аналітичних висновків. Основними моментами принципу є використання автоматизованих систем збору, які здатні сканувати великі обсяги відкритої інформації - від веб - ресурсів і соціальних мереж до форумів і баз даних. Важливу роль відіграє попередня фільтрація отриманих матеріалів, що передбачає очищення від дублікатів, неактуального або спам - контенту, а також технічних шумів.

До принципу можна віднести такі інструменти, як Scrapy, Twint, CrowdTangle, Dataminr та ESPY, які забезпечують швидкий пошук і збір відкритих даних у реальному часі та створюють основу для подальшого аналітичного опрацювання.

2. Принцип аналітичної обробки текстової інформації передбачає використання технологій обробки природної мови (Natural Language Processing, NLP) для інтерпретації змісту текстів з відкритих джерел - новинних порталів, соціальних мереж, публічних документів чи форумів. Даний принцип спрямований на виявлення смислових зв'язків, емоційних відтінків, тематики й потенційних маніпуляцій у текстових повідомленнях. Ключовими моментами є класифікація текстів за темами, виявлення ключових осіб та локацій, аналіз тональності й побудова контекстних моделей для подальшої перевірки достовірності.

До цього принципу належать такі інструменти, як GPT - 4, BERT, SpaCy та HuggingFace Transformers, які забезпечують високоточний семантичний аналіз великих обсягів текстової інформації й допомагають автоматизувати пошук закономірностей і фейкових наративів.

3. Принцип візуального аналізу базується на застосуванні технологій комп'ютерного зору (Computer Vision, CV) для розпізнавання, ідентифікації та класифікації об'єктів на зображеннях, у відео чи супутникових знімках. Цей принцип дозволяє отримувати візуальні докази, що доповнюють або підтверджують текстову інформацію, а також визначати геолокацію, типи об'єктів і їхню динаміку у просторі. Ключовими моментами є автоматичне визначення об'єктів, аналіз метаданих, відновлення контексту подій і просторових взаємозв'язків між об'єктами.

До даного принципу належать інструменти OpenCV, TensorFlow Object Detection, Ovis 1.6 Gemma 2 - 9B, CarNet.ШІ та Google Vision API, які забезпечують обробку великих обсягів зображень і відео, а також дозволяють точно встановлювати місце, час і характер подій.

4. Принцип перевірки достовірності та протидії дезінформації спрямований на оцінку надійності зібраних даних і виявлення можливих маніпуляцій, фальсифікацій або ознак редагування матеріалів. Його реалізація є важливою складовою OSINT - досліджень, оскільки саме на цьому етапі здійснюється підтвердження правдивості зображень, відео чи текстових повідомлень. Основними моментами є перевірка джерел і метаданих, аналіз цифрових слідів редагування, виявлення deepfake - технологій, а також перехресна перевірка інформації з різних платформ.

Прикладами описаного принципу є інструменти Sensity, Reality Defender та Read Their Lips, що забезпечують автоматичну перевірку візуального й аудіоконтенту, визначають ознаки монтажу та допомагають підвищити достовірність.

5. Принцип представлення результатів передбачає узагальнення та подання результатів аналітичної діяльності у зручній для сприйняття формі. Він реалізується через побудову інтерактивних графів, мережевих карт, аналітичних панелей або звітів, які відображають зв’язки між об’єктами, тенденції чи часову динаміку подій. Ключовими моментами є інтеграція даних із різних джерел, використання візуальних інструментів для пошуку прихованих закономірностей і формування цілісної картини дослідження.

До цього принципу належать інструменти Maltego, Palantir Foundry, Gephi, Kibana та Power BI, які дозволяють ефективно візуалізувати результати аналітики й забезпечують зручне представлення інформації для подальшого ухвалення рішень.

6. Принцип інтеграції та автоматизації OSINT - процесів є узагальнювальним і спрямований на об’єднання всіх етапів аналітичного циклу в єдину технологічну систему. Його сутність полягає у створенні інтегрованих платформ або персональних ШІ - асистентів, які здатні виконувати кілька функцій одночасно - від збору та аналізу до верифікації й візуалізації результатів. Основними моментами цього принципу є взаємодія

між різними типами інструментів, автоматизація повторюваних завдань і можливість адаптації системи під конкретні цілі дослідження.

До даного принципу належать ChatGPT, AutoGPT, HuggingFace Agents та Palantir Foundry, які забезпечують створення комплексних інтелектуальних рішень, здатних підтримувати аналітика на всіх етапах OSINT - дослідження.

Для практичної реалізації розроблених критеріїв та функціональних принципів доцільно здійснити систематизацію наявних ШІ - інструментів, що використовуються в OSINT - дослідженнях. Така класифікація дає змогу не лише впорядкувати технологічні засоби за їх функціональним призначенням, а й виявити їхні взаємозв'язки з основними етапами аналітичного процесу - від збору інформації до верифікації та візуалізації результатів.

Подана нижче систематизація відображає основні категорії сучасних ШІ - інструментів, які інтегруються в OSINT - аналітику. Вона базується на функціональному підході, де кожна категорія інструментів відповідає певній частині OSINT - циклу (збір, аналіз, перевірка, представлення). Представлені приклади демонструють практичні можливості кожної групи - від інструментів первинного збору до інтелектуальних асистентів, що забезпечують автоматизацію процесу.

Для наочності та систематизації наведемо основні категорії інструментів разом із прикладами та ключовими особливостями у вигляді таблиці 2.1.

Таблиця 2.1 - Категорії ШІ - інструментів для OSINT та приклади їх застосування.

| Категорія інструментів | Функціональне призначення | Приклади ШІ - інструментів | Особливості застосування |
|---|---|---|---|
| Автоматизований збір та попередня фільтрація даних (ШІ - моніторинг) | ШІ - сканування соцмереж, потоків даних, виявлення аномалій та сигналів | Dataminr, ESPY (AI - OSINT платформа) | Використовують ML - моделі для аналізу великих потоків даних у реальному часі, NLP - виявлення тональності, загроз, патернів. |

| | | | |
|---|---|---|---|
| Аналітика зв’язків та мережевих структур (ШІ - graph intelligence) | Побудова ШІ - графів, автоматичний пошук зв’язків між сутностями | Palantir Foundry (AI - pipeline), Skopenow AI | Використовують ML - алгоритми для ідентифікації прихованих зв’язків, |

| | | | |
|---|---|---|---|
| | | | класифікації об’єктів, пріоритетизації ризиків. |
| ШІ - NLP (обробка природної мови) | Семантичний аналіз текстів, класифікація, узагальнення, детекція аномалій | GPT - 4 / GPT - 5, BERT, ESPY NLP, SpaCy Transformer models | Генеративні та трансформерні моделі аналізують контент соцмереж, новини, документи, визначають фейки, стилістику, ключові сутності. |
| Комп’ютерний зір (ШІ - CV) | Розпізнавання об’єктів, моделей транспортних засобів, геолокація за зображеннями | Gemma 2 - 9B Vision, Google Vision AI, TensorFlow | Моделі виконують класифікацію об’єктів, визначають місцевість, читають текст, працюють із супутниковими знімками. |
| Біометричний аналіз / розпізнавання облич | Ідентифікація облич, пошук схожостей, порівняння з базами | FaceMatch AI, PimEyes, Clearview AI | Використовують глибоке навчання для верифікації особи, виявлення збігів, аналізу портретів та біометричних патернів. |
| ШІ - верифікація та протидія дезінформації | Виявлення deepfake, перевірка медіаконтенту, аналіз відео/аудіо | Sensity AI (ШІ - модулі), Reality Defender, Read Their Lips ШІ | Детектори deepfake, зміни пікселів, аналіз рухів облич, синтезованого голосу та підроблених відео. |
| Обробка та покращення якості зображень (ШІ - Enhancement) | Підвищення роздільності, очищення, відновлення деталей | Remini AI, Let’s Enhance AI, | Застосовують генеративні моделі для апскейлу, реконструкції низької якості, відновлення дрібних деталей. |
| ШІ - асистенти для OSINT | Автоматизація частини OSINT - процесів, створення персональних ШІ - помічників | ChatGPT, GPT - 4/5 Custom Assistants, HuggingFace Agents, AutoGPT | Забезпечують генерацію OSINT - запитів, фактчекінг, класифікацію, аналіз акаунтів, геолокацію, складання звітів. |

Класифікація ШІ - інструментів дає змогу візуалізувати логічну структуру аналітичного процесу OSINT та обґрунтувати вибір технологій залежно від типу завдань. Вона слугує методологічною основою для побудови моделі вибору оптимального набору інструментів, що буде розроблена у наступному підрозділі (2.2). Такий підхід дозволяє аналітику обирати не окремі продукти, а цілісні технологічні зв’язки - наприклад,

поєднувати

інструменти збору (Scrapy, ESPY) з модулями обробки даних (GPT - 4, BERT) чи верифікації ( Sensity).

Підсумовуючи вище зазначені функціональні принципи класифікації ШІ - інструментів відображають логіку аналітичного процесу OSINT, який реалізується через послідовні етапи, схематично зображено на рис. 2.1.

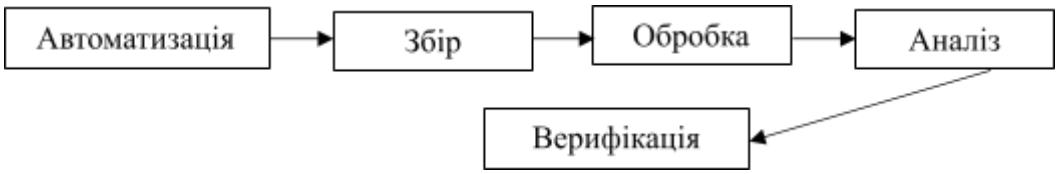


Рисунок 2.1 - Послідовність етапів OSINT - дослідження із застосуванням ШІ

Така системна побудова забезпечує цілісність дослідження, уможливлює вибір оптимального набору ШІ - рішень для конкретних завдань та створює основу для подальшої моделі автоматизованого вибору інструментів

## 2.2 Формування моделі вибору оптимального набору інструментів залежно від завдань дослідження

Практична реалізація розроблених критеріїв та функціональних принципів вимагає здійснення систематизації наявних ШІ - інструментів, які можна використовувати для проведення OSINT - дослідження. В першу чергу, сформована модель має на меті узгодити тип завдання з відповідним ШІ - інструментом. Це потрібно для того щоб уникнути дублювання функцій, а також оптимізувати послідовність використання інструментів на різних етапах аналітичного процесу. Крім того, модель покликана мінімізувати надлишок інструментів, адже на сучасному етапі розвитку штучного інтелекту існує значна кількість нейромереж, здатних швидко обробляти великі обсяги інформації, однак не всі вони забезпечують однакову якість, стабільність чи доступність функцій. Частина інструментів є комерційними або обмеженими

у використанні, що створює потребу в раціональному відборі оптимального набору ШІ - засобів відповідно до цілей дослідження.

Підсумовуючи, можна виокремити основний принцип моделі - базування на поетапній логіці, яка включає визначення типу завдання, ідентифікацію типу даних, оцінку рівня автоматизації, підбір відповідних технологій та оцінку їх ефективності та сумісності. Модель має на меті створенні інтегрованого набору інструментів, що забезпечить повний цикл OSINT - аналізу - від збору інформації до її верифікації та представлення результатів.

Модель вибору оптимального набору ШІ - інструментів для OSINT базується на принципі функціональної відповідності (рис. 2.2).

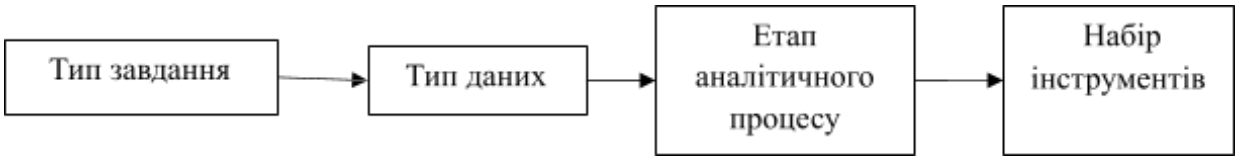


Рисунок 2.2 - Принцип функціональної відповідності для моделі вибору оптимального набору ШІ - інструментів для OSINT

Іншими словами, кожне завдання OSINT - дослідження класифікується за видом необхідних даних та етапом аналітики, що дозволяє визначити, які саме технологічні рішення (ШІ - інструменти) будуть найбільш доречними. Підсумовуючи все вище зазначене, можна сказати, що така методологічна вісь забезпечує системність і послідовність дій аналітика: від чіткого визначення цілей до автоматизованого отримання результату. Важливо підкреслити, що хоча загальний підхід моделі може застосовуватися й в інших сферах, даний підхід зосереджено саме на потребах OSINT. Це обумовлено специфікою відкритої розвідки, де обсяг публічних даних дуже великий, а також появою значної кількості згенерованого ШІ - контенту, який дедалі важче відрізнити від реального. Відтак, інтеграція штучного інтелекту в OSINT дає можливість підсилювати розслідування на різних етапах - від збору інформації до її верифікації - і значно розширює можливості дослідників.

Для практичної реалізації моделі було сформовано аналітичний каркас, який зіставляє типові OSINT - завдання з оптимальними видами ШІ - інструментів. У табл. 2.2 наведено матрицю відповідності, показуючи, які інструменти доцільно застосовувати для конкретного типу завдання на відповідному етапі розвідувального процесу.

Як висновок, можна припустити, що наведений перелік інструментів охоплює найбільш відомі та доступні рішення станом на 2024 - 2025 роки, які є популярними серед OSINT - дослідників. Це підтверджується публікаціями, де фігурують такі рішення, як Maltego, OVIS, Dataminr, Skopenow та інші, у якості ефективних ШІ - інструментів для відкритих розслідувань. Таким чином, модель спирається на перевірені часом та спільнотою технології, що забезпечує її практичну цінність.

Таблиця 2.2 - Матриця відповідності завдань OSINT та типів ШІ - інструментів

| Тип завдання OSINT - дослідження | Тип даних | Етап аналітичного процесу | Рекомендовані ШІ - інструменти | Очікуваний результат |
|---|---|---|---|---|
| ШІ - інструмент для проведення OSINT - дослідження | Пошук, зображення, текстові. | Збір та пошук | Artellence | Знаходження інформації |
| Моніторинг соціальних мереж та ЗМІ | Текстові, мультимедійні | Збір даних, попередня фільтрація | Twint, Dataminr, CrowdTangle | Виявлення тенденцій, ключових джерел, настроїв аудиторії |
| Аналіз контенту публікацій та виявлення дезінформації | Текстові | NLP - аналіз, фактчекінг | GPT - 4, BERT, SpaCy | Виокремлення ключових слів, тем; виявлення фейкових наративів |
| Ідентифікація об’єктів на фото та відео | Зображення, відео | Візуальний аналіз (CV) | OpenCV, OVIS 1.6, CarNet.ШІ | Розпізнавання об’єктів, типів техніки; визначення геолокації |
| Перевірка достовірності матеріалів | Мультимедійні (відео, аудіо) | Верифікація (автентифікація) | Sensity ШІ, Reality Defender | Виявлення ознак монтажу, редагування; розпізнавання deepfake - контенту |
| Геолокаційний аналіз і картографування | Геопросторові дані | Інтеграція та візуалізація | Maltego, Palantir | Встановлення місцезнаходжень, маршрутів; |

| | | | | |
|---|---|---|---|---|
| | | | Foundry, Google Earth | побудова просторових зв’язків |
| Підготовка комплексного OSINT - звіту | Усі типи даних | Автоматизація (узагальнення) | ChatGPT, AutoGPT, HuggingFace Agents | Автоматизоване узагальнення результатів і формування підсумкового звіту |

Таким чином, порівняння різних завдань і рішень дозволяє побачити логіку побудови комплексу засобів: наприклад, для моніторингу соцмереж обрано інструменти, що автоматизують збір публікацій та сигналів з Twitter і новин (Twint, Dataminr тощо) - ці сервіси забезпечують реальний час відстеження та оповіщення про нові дані. Натомість для контент - аналізу текстів доцільно застосовувати мовні моделі (LLM та трансформери), які здатні виділяти ключові ідеї й тональність повідомлень без ручного перегляду текстів.

У випадку аналізу зображень/відео, перевага надається комп’ютерному баченню: зокрема, інструмент OVIS 1.6 спеціалізується на розпізнаванні об’єктів та описі місцевості на фото/відео, а CarNet.ШІ визначає марку і модель автомобіля з точністю ~97%, що особливо цінно для військових OSINT

- досліджень. Для верифікації достовірності мультимедійних матеріалів використовуються інструменти на кшталт (плагін для перевірки відео та зображень) і платформи для детектування діпфейків Sensity та Reality Defender. Вони дозволяють автоматично виявляти синтетичний або змінений контент за допомогою аналізу піксельних артефактів, невідповідностей звуку/відео тощо.

Геопросторові завдання (геолокація та картографування) потребують інтеграції різнорідних даних і їхнього візуального представлення; тут оптимальними є Maltego (потужний засіб для побудови графів зв’язків і картографування даних) та Palantir Foundry (платформа корпоративного рівня, що агрегує дані з різних джерел і застосовує ML для пошуку шаблонів). Нарешті, завершальний етап - підготовка звіту - доцільно автоматизувати за

допомогою генеративних моделей (таких як ChatGPT, AutoGPT). Вони здатні швидко узагальнювати великі обсяги зібраної інформації та формувати структурований аналітичний звіт мовою, зрозумілою замовнику. Зокрема, інтеграція ChatGPT у процес OSINT вже використовується для генерування довідкової інформації, списків ключових термінів і навіть підготовки чернеток текстів для Human Intelligence (HUMINT) спілкування.

У результаті проведеного порівняння типів завдань та інструментів можна зробити висновок, що запропонований набір ШІ - рішень покриває повний цикл OSINT: від збору даних до їх аналізу, перевірки та представлення. Кожен із рекомендованих інструментів обраний з огляду на його ефективність, актуальність та широке застосування в спільноті OSINT - дослідників, що підтверджує його оптимальність для відповідної підзадачі.

Для обґрунтування вибору конкретних інструментів доцільно оцінити їх за низкою критеріїв. Таблиця 2.3 наводить порівняльну характеристику рекомендованих ШІ - інструментів за показниками рівня автоматизації, швидкості роботи, точності аналізу, масштабованості та доступності. Таке порівняння висвітлює сильні сторони кожного рішення та допомагає пояснити, чому саме цей інструментарій вважається оптимальним.

Таблиця 2.3 - Порівняльна оцінка ефективності та можливостей ШІ - інструментів для OSINT

| Інструмент | Тип даних | Рівень автоматизації | Швидкість | Точність | Масштабованість | Доступність |
|---|---|---|---|---|---|---|
| GPT - 4 | Текст | Часткова (потрібен prompt) | Висока | Дуже висока | Висока | Частково платна (API) |
| | Відео, зобр. | Часткова (плагін) | Середня | Висока | Середня | Безкоштовна |
| OpenCV | Зображення, відео | Повна (скрипти CV) | Висока | Висока | Висока | Безкоштовна (open - source) |
| Dataminr | Текст (соцмережі) | Повна (real - time ШІ) | Висока | Висока | Висока | Комерційна ( SaaS ) |

| | | | | | | |
|---|---|---|---|---|---|---|
| Palantir Foundry | Усі (інтегр. платформа) | Інтегрована (енд - ту - енд) | Висока | Висока | Дуже висока | Комерційна (Enterprise) |
| ChatGPT / AutoGPT | Текст, мультимодальні | Інтегрована (LLM - агент) | Висока | Висока | Висока | Частково платна |

Наведені оцінки базуються на відкритих характеристиках і емпіричних спостереженнях дослідників. Зокрема, GPT - 4 як представник великих мовних моделей демонструє найвищу якість розуміння та генерації тексту (точність наближається до експертної), проте для його використання потрібна участь аналітика у формулюванні запитів (тому рівень автоматизації визначено як частковий). забезпечує напівавтоматичну перевірку відеоконтенту: аналітик ініціює перевірку, а інструмент виконує ряд спеціалізованих аналізів (фрагментація відео, зворотний пошук зображень, метадані тощо); швидкість обробки середня через необхідність послідовного аналізу кадрів, зате точність виявлення маніпуляцій досить висока.

OpenCV як бібліотека комп’ютерного зору працює на повністю автоматизованій основі (скрипти можуть обробляти тисячі зображень без втручання людини), характеризується високою швидкодією та точністю алгоритмів машинного зору; її відкритий код і безкоштовна ліцензія роблять інструмент доступним і надзвичайно масштабованим.

Dataminr та подібні системи реального часу використовують потокову аналітику даних з соцмереж і новин; вони повністю автоматизовані і здатні майже миттєво видавати попередження про загрози або тренди, працюючи у масштабі всього інтернету (що пояснює високу масштабованість). Ці рішення є комерційними SaaS - продуктами, тому потребують придбання ліцензії.

Palantir Foundry, будучи корпоративною інтеграційною платформою, забезпечує енд - ту - енд автоматизацію OSINT - процесу в межах організації: від збору великих обсягів різнорідних даних до застосування ML - аналізу і спільної роботи аналітиків. Її точність і швидкість залишаються високими навіть на «великих даних», а масштабованість практично необмежена за

рахунок хмарної архітектури; недоліком є закритість та висока вартість рішення (комерційна ліцензія).

ChatGPT/AutoGPT та інші агентні LLM - системи забезпечують інтегровану автоматизацію: вони можуть самостійно виконувати низку послідовних кроків (наприклад, зібрати дані, проаналізувати та скласти текстовий звіт), однак іноді потребують нагляду людини для коригування напрямку роботи. Швидкість генерування відповіді у них висока (секунди чи хвилини на задачі, що вимагали б годин ручної роботи), точність залежить від якості навчання моделі і зазвичай достатньо висока для чернетки звіту. Доступ до таких моделей часто частково платний: базова версія ChatGPT може бути безкоштовною, але професійні функції (більший контекст, підключення до інтернету, спеціалізовані агенти) - за підпискою або через API.

Таким чином, порівняння за критеріями ефективності дозволило виявити, що обрані інструменти доповнюють один одного: безкоштовні рішення (OpenCV, ) можуть виконувати вузькі задачі з високою точністю, тоді як комерційні платформи (Dataminr, Palantir) забезпечують масштабність і швидкість на рівні великого потоку даних. У результаті, збалансований набір із цих інструментів дає змогу охопити різні аспекти OSINT з оптимальною продуктивністю.

На основі розробленої матриці відповідності та проведеної оцінки ефективності можна сформувати алгоритм дій аналітика для вибору оптимального інструментарію. Алгоритм відображає послідовність етапів, які забезпечують логічно обґрунтований вибір ШІ - засобів під конкретне OSINT - дослідження. Таким чином, процес побудови оптимального набору інструментів включає такі кроки:

1. Визначення цілей та типу завдання, даний процес полягає у тому щоб чітко формулювати мету розслідування і його категорії (наприклад, моніторинг соцмереж, ідентифікація об’єктів, перевірка фактів, тощо). Від правильного визначення завдання залежить подальший вибір методів і даних.

2. Встановлення типу необхідних даних, на цьому етапі аналітик з’ясовує, які саме дані потрібні для виконання завдання - текстові повідомлення, зображення, відео, геолокаційні дані, бази даних тощо. Тип даних визначає вибір інструментів (наприклад, для текстів - NLP - моделі, для зображень - CV - модулі).

3. Визначення етапу OSINT - процесу, етап полягає у тому щоб співвіднести завдання із фазою розвідувального циклу: збір інформації, її обробка/аналіз, верифікація (перевірка достовірності) чи візуалізація та звітування. Це звужує коло інструментів до тих, що призначені для конкретного етапу.

4. Підбір кандидатних ШІ - інструментів, тобто користуючись класифікацією з таблиці 2.2 (а також з огляду на доступні ресурси), обираються інструменти, що відповідають типу завдання, виду даних та етапу аналізу. Наприклад, якщо завдання - верифікація відео, то відповідні інструменти - яких достатньо для аналізу метаданих та ключових кадрів, або Sensity для глибшого аналізу на наявність діпфейку.

5. Оцінка ефективності та доступності полягає, що для кожного кандидатного інструменту проводиться оцінка за критеріями, чи достатня точність для даного кейсу, чи впишеться швидкодія в дедлайни, чи масштабоване рішення під обсяг даних, і чи є необхідні ліцензії/доступ. У результаті проведеного порівняння на цьому кроці відбираються найкращі претенденти - ті, що отримали найвищі оцінки та відповідають обмеженням проєкту (наприклад, бюджет або наявність експертизи для роботи з інструментом).

6. Формування інтегрованого пайплайна (набору інструментів), тобто обрані інструменти комбінуються у послідовність, що забезпечує повний цикл аналізу. Наприклад, пайплайн може включати: Twint для збору твітів - GPT - 4 для їхньої тематичної класифікації - OpenCV для аналізу зображень, знайдених у твітах - для перевірки відео - ChatGPT для зведення отриманих інсайтів у звіт. На цьому етапі також налаштовуються точки

інтеграції між інструментами (формати даних, API, скрипти автоматизації), щоб забезпечити безшовну передачу результатів від одного етапу до наступного.

7. Тестування і адаптація моделі, мається на увазі що перед повномасштабним застосуванням рекомендується перевірити збудований набір інструментів на тестових даних або в обмеженому обсязі реального кейсу. За підсумками тестування можливе коригування вибору інструментів (наприклад, заміна моделі на точнішу або додавання ще одного засобу для покриття пропусків). Така гнучка адаптація дозволяє підвищити надійність моделі під специфіку конкретного дослідження.


Рисунок 2.3 - Блок - схема прийняття рішень під час вибору ШІ - інструментів для OSINT - дослідження

На рис. 2.3 схематично зображено блок - схему прийняття рішень: починаючи від типу завдання, аналітик визначає відповідний тип даних, потім переходить до визначення етапу OSINT, після чого здійснюється підбір інструментів. Далі блок оцінки ефективності фільтрує вибрані інструменти за

якісними критеріями, і на виході формується оптимальний набір. Завершальний блок відображає отриманий результат OSINT - дослідження. У схемі простежується послідовний причинно - наслідковий зв’язок, полягає від завдання - до даних, від даних - до методів, від методів - до конкретних технологічних рішень та фінального аналітичного продукту.

Підсумовуючи все вищезазначене, розроблена модель вибору оптимального набору ШІ - інструментів для OSINT - досліджень дозволяє системно узгодити аналітичні завдання із відповідними технологічними рішеннями. Її застосування забезпечує логічну послідовність дій і усуває дублювання функцій на різних етапах, що, своєю чергою, сприяє оптимізації часу аналізу. Як висновок, можна стверджувати, що запропонований підхід підвищує точність отримуваних розвідувальних даних, оскільки кожен інструмент використовується за призначенням (відповідно до своєї сильної сторони) і доповнює інші. Таким чином, модель створює основу для впровадження комплексної методики застосування ШІ в OSINT.

## 2.3 Покрокова розробка методики практичного застосування ШІ, що включає етапи

Розвиток технологій штучного інтелекту зумовив суттєве вдосконалення методів розвідки з відкритих джерел (OSINT), що дало можливість підвищити швидкість, точність та системність аналітичних досліджень. У рамках дослідження важливим етапом було охарактеризувати практичні підходи до інтеграції інструментів штучного інтелекту в процес проведення OSINT - дослідження, визначивши логіку їх застосування та послідовність реалізації аналітичних процедур.

Розроблена методика базується на принципах, викладених у попередніх підрозділах, зокрема на класифікації ШІ - інструментів за функціональними характеристиками та моделі їх оптимального добору відповідно до типів аналітичних завдань. Запропонований підхід передбачає послідовне

використання інструментів штучного інтелекту на кожному етапі дослідження - від постановки завдання й формування аналітичного запиту до підсумкової інтерпретації та представлення результатів.

Особливістю методики є її системна побудова, що забезпечує логічну взаємопов'язаність етапів аналітичного циклу та створює цілісну структуру обробки відкритих даних. Запропонована модель спрямована на оптимізацію аналітичного процесу, підвищення ефективності використання даних, а також забезпечення відтворюваності результатів за рахунок уніфікації процедур збору, аналізу, верифікації та візуалізації інформації.

### 2.3.1 Етап 1: Формалізація аналітичного запиту та визначення параметрів пошуку

Мета і межі дослідження. Перший крок - чітко сформулювати мету OSINT - розслідування та конкретні питання, на які потрібно отримати відповідь. Аналітик визначає аналітичний запит - описує, що саме слід розслідувати (подію, особу, об'єкт чи явище), а також окреслює межі дослідження - часовий період, географічний регіон, мови джерел тощо. Від правильності та деталізації цього формулювання залежить релевантність зібраної інформації на наступних етапах. Наприклад, якщо розслідується кібератака, варто зазначити її приблизний час, ціль, вид атаки; якщо аналізується персона - перелічити ключові факти біографії або сфери діяльності, які допоможуть звузити пошук. Чітке визначення рамок захищає від інформаційного «шума» надалі.

Далі аналітик встановлює критерії збору даних - набір початкових даних та фільтрів, за якими здійснюватиметься пошук. Сюди входять:

- Список ключових слів - основні та альтернативні (синоніми, різні написання імен, релевантні хештеги). Наприклад, для події «витік даних корпорації X» доцільно виписати назву корпорації, назву витоку (якщо відома), можливі хештеги, пов'язані з цією подією.

- Джерела даних - пріоритетні платформи або сайти, звідки черпатиметься інформація (соцмережі: Twitter/X, Facebook, Instagram; форуми; конкретні новинні сайти; публічні бази даних; реєстри тощо).

- Типи даних - які види контенту цікавлять (текстові повідомлення, новинні статті, зображення, відео, аудіо, документи PDF і т.д.).

- Фільтри для відсікання нерелевантного - наприклад, мовні або територіальні (пошук тільки українською і англійською; тільки в межах Європи), часові (публікації за останній рік), за доменом (.gov, .edu для офіційних джерел) чи форматом файлів (тільки зображення, тільки PDF). Грамотно задані параметри допомагають відразу відфільтрувати зайву інформацію.

Співвіднесення з типом OSINT - завдання. На цьому ж етапі важливо класифікувати поставлену проблему згідно з моделлю з підрозділу 2.2. Аналітик визначає, до якого типу OSINT - завдань належить розслідування (наприклад, моніторинг соцмереж, розслідування дезінформації, геолокація подій) і які типи даних переважатимуть. Це дозволяє планувати використання конкретних ШІ - інструментів наперед.

Якщо мета - виявити мережу контактів певної особи, то пріоритетними будуть соцмережі та бази даних із інформацією про її зв’язки, а з інструментів знадобляться системи аналізу соціальних графів (Maltego, Skopenow тощо).

Якщо дослідження стосується верифікації відео, вже на етапі планування варто передбачити застосування інструментів перевірки медіаконтенту (наприклад, плагін для ключових кадрів відео, платформа Sensity ШІ для детекції дипфейків) і виписати технічні дані відео (оригінальне джерело, дата зйомки, цифровий хеш файлу), щоб надалі використовувати їх у пошуку.

Залучення ШІ при плануванні. На цьому етапі аналітик може використати самі ШІ - технології як допоміжний засіб. Зокрема, великі мовні моделі (LLM) на кшталт ChatGPT корисні для генерації додаткових ідей: вони можуть запропонувати релевантні ключові слова та синоніми, про які

аналітик

міг не згадати, а також надати довідкову інформацію по темі запиту. Наприклад, сформулювавши в ChatGPT суть запиту, можна попросити модель згенерувати список 10 пов’язаних термінів чи хештегів, або коротко пояснити бекграунд події - це допоможе краще зрозуміти, де шукати. Важливо при цьому пам’ятати, що модель може помилятися: всю інформацію і терміни, підказані ШІ, слід перевірити вручну, щоб не внести на наступних стадіях хибні дані. Отже, вихідний продукт першого етапу - технічне завдання для систем збору, де прописано що шукати, де шукати і за якими критеріями відбирати потрібні дані.

### 2.3.2 Етап 2: Автоматизований збір даних і попередня фільтрація з використанням ШІ

На другому етапі здійснюється безпосередній збір інформації з відкритих джерел за заданими параметрами - максимально автоматизовано. Сучасні ШІ - інструменти та скрейпінгові утиліти дозволяють охоплювати великі масиви даних майже в реальному часі, мінімізуючи ручну роботу. Залежно від типу джерел застосовуються різні підходи:

- моніторинг соцмереж і стрічок новин. Для збору постів із соцмереж (Twitter/X, Facebook, Instagram тощо) використовуються спеціалізовані скрейпери та сервіси стрімінгу. Наприклад, Twint - інструмент для збору твітів без використання офіційного API - дозволяє автоматично витягнути твіти за вказаними ключовими словами, хештегами чи з конкретних акаунтів, з можливістю фільтрації за датою. Аналогічно CrowdTangle (від Meta) забезпечує моніторинг публікацій у Facebook/Instagram по заданій тематиці. Більш просунуті комерційні сервіси на кшталт Dataminr та ESPY мають вбудовані алгоритми ШІ, які в потоці соцмедійних даних виявляють тренди та аномальні сплески. Вони здатні цілодобово відстежувати тисячі джерел і надсилати сповіщення, щойно з’являється релевантна інформація (наприклад, повідомлення про надзвичайну подію). Для моніторингу

новинних сайтів, блогів і форумів часто застосовуються RSS - агрегатори або власні веб - краулери, створені на базі фреймворків на кшталт Scrapy (Python). Останні можна налаштувати як «павуків», що обходять вказані сайти і зчитують новий контент за визначеними правилами (наприклад, всі статті розділу «Новини» з фільтром по ключових словах у тексті).

- збір зі статичних веб - сторінок і баз даних. Якщо потрібно зібрати дані зі звичайних веб - ресурсів (наприклад, списки фірм, профілі осіб, записи реєстрів), налаштовуються скрипти парсингу HTML. Популярні утиліти: BeautifulSoup (для «вибірки» потрібних полів із HTML - коду) або хмарні сервіси типу Import.io для вилучення табличних даних. У разі роботи з відкритими базами (Whois, корпоративні реєстри тощо) - доступ через API сервісів або запити через спеціалізовані OSINT - платформи. ШІ - компоненти можуть допомагати і тут: деякі інструменти здатні динамічно знаходити нові посилання по ходу скрейпінгу. Наприклад, парсер тексту з алгоритмом машинного навчання може визначати, що на зібраній сторінці згадується інший релевантний об’єкт чи URL, і автоматично ставити його в чергу на обхід, розширюючи охоплення даних.

Попередня фільтрація (очищення даних). Масив сирих даних, зібраний на цьому кроці, зазвичай містить значну частку «шуму» - дублікати, нерелевантні записи, спам. Тому критично важливо виконати автоматизоване очищення перед глибинним аналізом:

1. Видалення дублікатів. За допомогою хешування контенту або простого порівняння текстів виявляються повтори однієї й тієї ж інформації (наприклад, передруки ідентичної новини різними сайтами, ретвіти) і залишаються тільки унікальні записи. Це запобігає «зсуву» статистики та дублюванню аналізу.

2. Фільтрація спаму та нерелевантного. Використовуються NLP - моделі класифікації, що автоматично оцінюють, чи належить текст до теми дослідження. Приміром, якщо ключове слово - назва організації «X», можна пропустити всі зібрані тексти через мовну модель (наприклад, BERT або

навіть GPT - 4), спеціально налаштовану класифікувати, чи текст стосується діяльності організації X. Повідомлення, де «X» згадується в іншому контексті, отримають низький рейтинг і будуть відсіяні. Так само можна відфільтрувати токсичний або рекламний контент: моделі sentiment analysis визначать тон повідомлення (нейтральний, негативний, позитивний) і при потребі можна відкинути, скажімо, надто емоційні пости, якщо завдання вимагає сухих фактів.

3. Нормалізація та структурування. Зібрані дані приводяться до уніфікованого вигляду. Після очищення інформація з різних джерел конвертується у зручний формат - наприклад, усі дані складаються у таблицю CSV або в базу даних із фіксованими полями: дата, джерело (URL), автор/акаунт, текст повідомлення/опис, додаткові атрибути (геолокація, хештеги тощо). Паралельно ШІ - алгоритми можуть виконати задачі на кшталт розпізнавання імен чи географічних назв у тексті для їх подальшої стандартизації (щоб різні варіанти написання одного місця чи прізвища звести до спільного ідентифікатора).

Результат другого етапу - сформована початкова вибірка даних, очищена від явного шуму і структурована для аналізу. Аналітик отримує скорочений, «знормалізований» набір матеріалу, який легше переглядати і в якому простіше застосовувати аналітичні алгоритми. Автоматизація збору та фільтрації суттєво економить час (години, а то й дні ручного перегляду відсіюються) і підвищує якість подальшого аналізу.

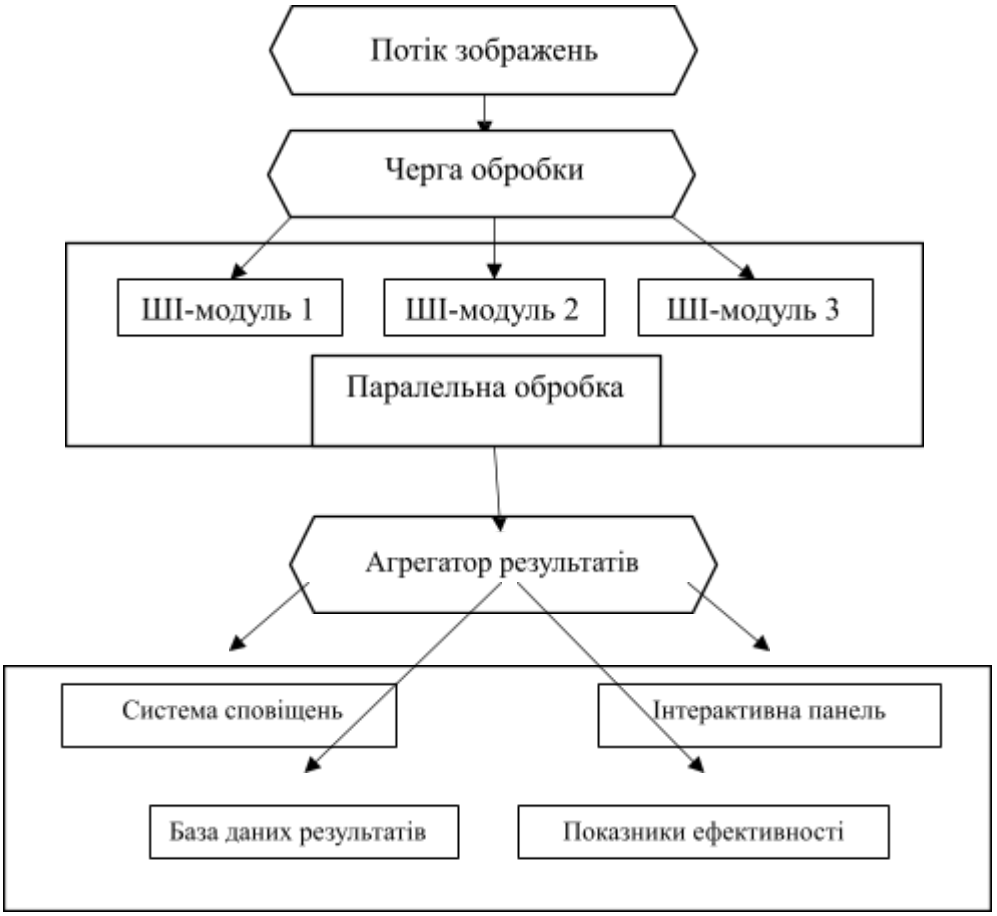


Рисунок 2.4 - Схема автоматизованого алгоритму обробки даних

Виходячи з рисунку 2.4, потік даних (наприклад, стрім зображень чи постів) надходить у чергу на обробку, після чого розпаралелюється між кількома ШІ - модулями (воркерами) для аналізу. Результати агрегуються та надходять до вихідних систем: баз даних, систем сповіщення, дашбордів тощо. Така архітектура дозволяє обробляти великі обсяги OSINT - даних у реальному часі завдяки паралельній роботі ШІ - модулів (аналіз тексту, зображень, класифікація).

### 2.3.3 Етап 3: Поглиблений аналіз даних за допомогою ШІ (геолокація, розпізнавання об'єктів, аналіз тональності)

Третій етап - це детальна аналітична обробка зібраної інформації з використанням інструментів ШІ. На цьому кроці від сирих даних потрібно отримати знання: смислові зв'язки, закономірності, факти, які відповідають на питання розслідування. Залежно від природи даних (текст, зображення, відео тощо) паралельно застосовуються різні ШІ - підходи:

Обробка текстів (NLP). До текстових даних (пости, статті, документи) застосовуються методи обробки природної мови. Перший підпроцес - семантичний аналіз: виявлення ключових тем, сюжетів та об'єктів у масиві текстів. Нейронні мовні моделі (BERT, RoBERTa, GPT - 4) можуть класифікувати тексти за темами або автоматично реферувати великі документи. Наприклад, маючи сотні твітів з етапу 2, аналітик може використати GPT - 4 для узагальнення - отримати стислий огляд, про що люди пишуть, які події згадуються найчастіше. Далі виконується видобування сутностей (Named Entity Recognition): за допомогою бібліотек на кшталт SpaCy або трансформерних моделей визначаються іменовані сутності - імена людей, організацій, локації, дати тощо. Це дозволить побачити, які персони чи місця найчастіше фігурують в контенті.

Наступний аспект - аналіз тональності та емоційного забарвлення текстів. Спеціалізовані моделі (VADER, RoBERTa Sentiment або GPT - додатки) визначають, чи є текст негативним, позитивним чи нейтральним. Це особливо важливо, якщо треба зрозуміти реакцію аудиторії на подію (наприклад, переважає схвалення чи обурення). Потокове відстеження трендів також можливе: ШІ може моніторити соцмережі в реальному часі і визначати зміну настроїв або виявляти сплеск обговорення певних тем. Окрім того, NLP - алгоритми допомагають виявляти аномалії та приховані наративи - наприклад, знайти не типові для основного інформаційного фону

повідомлення (що може свідчити про інформаційну атаку), або виявити повторювані фрази і меседжі, характерні для координованих кампаній.

Аналіз зображень та відео (Computer Vision). Візуальні дані, зібрані на попередньому етапі (фотографії, скриншоти, відеокадри, карти), обробляються методами комп'ютерного зору. Основне завдання - розпізнавання об'єктів і сцен.

Для OSINT часто критично розпізнати специфічні об'єкти, наприклад, військову техніку за фото. Існують спеціалізовані моделі: інструмент OVIS 1.6 (Gemma 2 - 9B) навчений детально описувати сцени та об'єкти, а сервіс CarNet.ШІ розпізнає марки і моделі автомобілів. Таким чином, зі знімка можна автоматично отримати текстовий опис: «на фото танк Т - 72 і двоє військових» або «червоний седан Toyota Camry з пошкодженим бампером». Ця інформація співставляється з іншими даними розслідування для підтвердження чи спростування гіпотез.

Важливою підзадачею є геолокація - встановлення місця, де було зроблено фото чи відео. ШІ допомагає двома шляхами. Перший - аналіз самого зображення на наявність відомих орієнтирів або характерних ознак місцевості. Наприклад, модель CV може розпізнати на фоні Ейфелеву вежу або собор, тоді місце зйомки очевидне. Якщо прямих орієнтирів нема, алгоритм оцінює ландшафт, архітектуру, рослинність: ці дані потім звіряються з картографічними сервісами (Google Earth, Яндекс Панорами) - часто так знаходять точне місце. Другий шлях - використання метаданих файлів. ШІ - скрипти автоматично витягають EXIF - дані фото, де можуть бути GPS - координати або модель камери і час зйомки. За знайденими координатами точка автоматично позначається на карті і перевіряється на відповідність тому, що видно на фото (наприклад, чи співпадає пейзаж). У випадку відео застосовується аналіз по кадрах: за допомогою CV можна відстежувати рух об'єктів у часі, будуючи їх маршрут, або синхронізувати декілька відео одного інциденту (якщо на них ті самі об'єкти зняті під різними кутами).

Для біометричних задач (розпізнавання облич) залучаються окремі сервіси. Сучасні алгоритми глибинного навчання ідентифікують обличчя з високою точністю за наявності зразків для порівняння. Інструменти на кшталт PimEyes чи Clearview ШІ (обмежений в багатьох країнах) виконують пошук по базах зображень в інтернеті, щоб знайти інші фото тієї ж людини. У OSINT це допоможе встановити особу людини на анонімному фото, якщо її раніше публікували. Інший підхід - сервіси на кшталт Face Match, що порівнюють два наданих зображення і видають відсоток схожості, а також приблизний вік та стать особи. Така перевірка корисна, щоб підтвердити, що на двох різних знімках одна й та ж людина.

Ще один вид автоматизованої обробки - покращення якості зображень. Часто аналітик має справу з неякісними, низької роздільності фото (наприклад, кадри з камери спостереження або скріншоти перепостів). Щоб витягти більше деталей, використовуються нейромережеві інструменти підвищення роздільності (так звані super - resolution). Наприклад, сервіси ШІ Image Enlarger, Let’s Enhance ШІ, Remini збільшують зображення в 2 - 4 рази, доматовуючи пікселі на основі навченої моделі. У результаті розмитий номерний знак може стати читабельним, а нечіткий шеврон на формі - розпізнаваним. Хоча такі алгоритми не створюють справжніх нових деталей (лише інтерполюють існуючі), вони суттєво підвищують успіх наступного розпізнавання об’єктів чи облич на покращених зображеннях.

Результати етапу 3 - перетворення неструктурованих даних у змістовну інформацію. Тексти трансформуються у набори фактів, списки виявлених осіб, таблиці подій; зображення та відео - у переліки розпізнаних об’єктів, встановлених місць, відстежених переміщень. Часто ці результати оформлюються як проміжні артефакти: наприклад, електронна карта з позначками всіх встановлених локацій, граф зв’язків між фігурантами, діаграма тональності відгуків.

На цьому етапі аналітик вже може робити попередні висновки. Однак, перш ніж виносити їх на розсуд замовника або публіки, треба переконатись у їх достовірності - цим займемося на наступному етапі.


Рисунок 2.5 - Алгоритмічна модель аналізу зображень за допомогою ШІ

Таким чино, спираючись на рис. 2.5, можна зробити наступне припущення, що вхідне зображення проходить через блок попередньої обробки (вирівнювання кольору, шумозаглушення), далі витягуються різні типи ознак: текстурні, колірні, формені. Ці ознаки подаються на вхід ШІ - моделі (нейронної мережі), яка аналізує їх і виконує класифікацію - наприклад, визначає матеріал чи об’єкт на зображенні. На виході отримуємо результат аналізу (ідентифікований об’єкт або віднесення до категорії). Подібні конвеєри застосовуються і для інших задач: розпізнавання облич, визначення локації за зображенням тощо.

Нижче в табл. 2.4 наведено основні типи ШІ - інструментів, які застосовуються на етапах 2 - 3 OSINT - цикла, з прикладами та типовим використанням.

Таблиця 2.4 - Основні типи ШІ - інструментів, які застосовуються на етапах 2 - 3 OSINT - цикла, з прикладами та типовим використанням.

| Категорія ШІ - інструментів | Приклади | Застосування в OSINT - дослідженнях |
|---|---|---|
| Моніторинг соцмедіа | Twint, CrowdTangle, Dataminr, ESPY | Автоматичний збір постів за ключовими словами, відстеження трендів і аномалій у реальному часі (сповіщення про події). |
| Визначення локації | earthkit.app | Даний інструмент дозволяє визначати локацію за фотографією. |
| NLP - аналіз текстів | BERT, GPT - 4, sentiment analysis models | Класифікація текстів за темами, узагальнення документів, виділення сутностей; визначення тональності публікацій (позитив/негатив) для оцінки реакції аудиторії. |
| Комп'ютерний зір (CV) | OVIS, YOLOv5, CarNet.ШІ, FaceMatch | Розпізнавання об'єктів на фото (техніка, люди, транспорт) та опис сцени; ідентифікація автомобілів за фото (марка/модель); порівняння облич або пошук профілів за зображенням людини. |
| Підвищення якості зображень | ШІ Image Enlarger, Remini | Машинне масштабування та очищення фото низької якості; покращення деталізації (номери авто, обличчя) для подальшого розпізнавання. |
| Верифікація контенту | (плагін), Sensity ШІ, Reality Defender | Зворотний пошук зображень і кадрів відео для виявлення першоджерел; визначення маніпуляцій на рівні пікселів, виявлення дипфейків та штучно згенерованого медіа (аналіз артефактів згенерованого зображення/аудіо). |
| Візуалізація і графовий аналіз | Maltego, Palantir Foundry | Побудова графів зв'язків між об'єктами (люди, компанії, домени) автоматично на основі даних; інтерактивні карти та панелі (дашборди) для геоприв'язаних подій; виявлення прихованих зв'язків через спільні атрибути. |
| LLM - асистенти | ChatGPT (Intel Assistant), Bing Chat ШІ | Генерація довідкової інформації про осіб, події, локації; пропозиція релевантних ключових термінів і хештегів для розширення пошуку; автоматизоване створення чорнових аналітичних звітів і висновків на основі зібраних даних (з подальшим редагуванням людиною). |

Виходячи з даних наведеної таблиці можна зробити висновок, що сучасні ШІ - інструменти охоплюють ключові задачі етапів 2–3 OSINT - цикла

- від збору та структуризації даних до їх аналітичної інтерпретації. Вони дозволяють автоматизувати рутинні процеси, підвищують точність верифікації інформації, розширюють можливості дослідника у роботі з

великомасштабними масивами даних та забезпечують більш глибоке й багатовимірне розуміння цифрових слідів об’єктів розслідування.

### 2.3.4 Етап 4: Верифікація та оцінка достовірності даних (протидія дезінформації і «deepfake»)

Четвертий етап присвячений перевірці правдивості та надійності отриманої на попередніх стадіях інформації. В епоху, коли значна частина контенту може бути згенерована або змінена ШІ (фейки, дипфейки), верифікація є надзвичайно важливою для забезпечення достовірності аналітичних висновків. Алгоритм дій на цьому етапі охоплює перевірку текстових даних, медіафайлів та виявлення можливих маніпуляцій.

Фактчек текстової інформації. Аналітик переглядає ключові факти і твердження, виявлені на етапі 3, і перехресно їх перевіряє у незалежних джерелах. Для цього використовуються звичайні пошукові системи та спеціальні бази даних фактів. ШІ може допомогти, наприклад, у вигляді семантичного пошуку схожих тверджень: існують моделі, що дозволяють порівняти речення з великою базою знань (Вікіпедія, фактчек - сайти) і знайти, чи згадувався подібний факт раніше. Деякі сучасні LLM навіть навчаються визначати правдоподібність тексту за стилістичними ознаками, але повністю покладатися на таку оцінку не можна - це лише підказка, яку аналітик перевіряє самостійно. Якщо є підозра, що певні пости у соцмережах згенеровані ботами або ІІ, застосовуються інструменти на кшталт Botometer: вони аналізують поведінкові шаблони акаунтів (частота постингу, шаблонні фрази, час активності) і виставляють бал «штучності». Високий бал може бути підставою відкинути інформацію від цього джерела або принаймні віднестися до неї з обережністю.

Для медіа - контенту існує цілий набір прийомів та інструментів. Перший крок - зворотний пошук зображень. Береться отримане на етапі 3 фото (або кадр з відео) і через сервіси Google Images, TinEye, Yandex Images

шукається, де і коли воно з’являлось раніше. Знайдений контекст часто викриває фейк. Наприклад, «сенсаційне» фото з війни може виявитись кадром трирічної давнини з кінофільму. Для спрощення цієї роботи використовують плагіни типу або WeVerify - вони можуть автоматично витягти ключові кадри з відео, збільшити їх та запустити по декількох пошукових системах одночасно.

Другий напрям - цифрова судова експертиза зображення: аналіз метаданих та пошук слідів редагування. Спеціальні програми (Exiftool, Fotoforensics) перевіряють, чи не було змінено EXIF - метадані (підозрілі ознаки - відсутність інформації про камеру, нереалістична дата зйомки). Алгоритм Error Level Analysis будує теплову карту зображення для виявлення областей, які відрізняються за ступенем стиснення - такі області могли бути вставлені з іншого зображення. Якщо на фото тіні від об’єктів падають під різними кутами або розмиття фону навколо вирізаної фігури виглядає неприродно - це ознаки підробки. Нейронні мережі також навчаються розпізнавати характерні артефакти від генеративних моделей (наприклад, спотворення текстур облич або несправжні відблиски в очах).

Окремий виклик - deepfake (підроблені відео або аудіо, створені генеративними мережами). Для їх виявлення існують такі інструменти, як Sensity ШІ (платформа моніторингу дипфейків) та Reality Defender. Платформа Sensity спеціалізується на розпізнаванні підроблених облич у відео та імітованого голосу, використовуючи комплексні моделі, що аналізують сотні ознак обличчя і голосу. Reality Defender діє як багаторівневий фільтр для медіа: завантаживши зображення чи відео, користувач отримує оцінку, наскільки великий шанс, що контент було згенеровано ШІ. Такі сервіси сканують цифрові артефакти, які залишають алгоритми генерації, - наприклад, невидимі для очей повторювані и шуму, спотворення на межах об’єктів, неузгодженість між рухом губ і звуком тощо. Інструмент Read Their Lips допомагає перевірити відео без звуку: він «читає» слова по руху губ на відео і

виводить текст - якщо текст не збігається з озвученим (або очікуваним) змістом, значить, аудіодоріжку підмінено.

Оцінка надійності та документування. Після технічних перевірок аналітик формує загальну оцінку достовірності кожного фрагмента даних. Частину матеріалів може бути повністю відбраковано (якщо, скажімо, встановлено штучне походження фото чи брехливість джерела). Інші дані отримують «мітки довіри» - наприклад, шкала від 1 до 5 або градація «непідтверджене», «підтверджене частково», «надійне». В аналітичних звітах бажано прямо вказувати, які факти підтверджені кількома джерелами, а які - ні. Використання ШІ на цьому етапі значно прискорює процес: те, що вручну могло зайняти багато годин (пошук джерел фото, покадровий аналіз відео, перевірка сотень постів), ШІ - інструменти виконують за хвилини. Проте остаточне рішення про довіру до інформації завжди приймає людина. Результат четвертого етапу - високоякісний набір перевірених розвідувальних даних, які з великою ймовірністю відповідають дійсності і можуть лягти в основу підсумкового аналізу.

### 2.3.5 Етап 5: Візуалізація, узагальнення та представлення результатів

Завершальний етап методики зосереджується на узагальненні та донесенні отриманих висновків у зручній для замовника формі. Попри те, що основну аналітичну роботу вже виконано на попередніх кроках, правильне оформлення результатів критично важливе: від цього залежить, чи будуть вони зрозумілі і переконливі для аудиторії (керівництва, клієнта або широкого загалу).

Багато інсайтів OSINT зручніше сприймати графічно, ніж у вигляді тексту. Тому аналітик на основі перевірених даних створює наочні матеріали за наступною послідовністю.

Графи зв’язків, мається на уваззі, якщо розслідування виявило зв’язки між суб’єктами (особами, компаніями, об’єктами), доцільно подати це як граф. Вузли графа позначають суб’єкти, лінії - типи зв’язків (дружні стосунки, спільне місце роботи, транзакції, спільний номер телефону тощо). Будувати графи можна у спеціалізованих інструментах (Maltego, i2 Analyst’s Notebook) або навіть у Python - бібліотеках (NetworkX) з подальшим експортуванням. На графі одразу видно «центральні вузли» (хто має найбільше зв’язків) і опосередковані зв’язки (через кого дві особи непрямо пов’язані). Maltego особливо зручний, бо може сам підтягувати дані з інтернету по заданих сутностях і розширювати граф напівавтоматично. У результаті виходить наочна схема, яка часто є ключовою для OSINT - звітів (наприклад, схема зв’язків між фірмами - прокладками, через які відмивались кошти).

Карти та географічні діаграми, коли дані прив’язані до місць, використовується картографічна візуалізація. На електронній карті (Google Maps, QGIS) позначаються ключові точки: місця подій, координати фотографій, маршрути переміщень. Це дозволяє виявити просторові шаблони

- скажімо, концентрацію інцидентів у певному регіоні, або шлях об’єкта розслідування. Сучасні інструменти (наприклад, платформа Palantir Foundry) дозволяють будувати інтерактивні карти, де при натисканні на точку відкриваються додаткові дані (фотографії з цього місця, опис події тощо). Такі візуалізації надзвичайно переконливі для демонстрації, адже «карта не бреше»
- глядач сам бачить географію явища.

Хронології та графіки, для аналізу розвитку подій у часі створюють стрічки часу (timeline) або графіки. Стрічка часу являє собою вісь, де нанесено послідовно всі події з короткими описами і датами - наочно показує, що за чим відбулось. Якщо ж важлива динаміка показників (наприклад, кількість згадок теми по місяцях), будують лінійний графік або гістограму. Ілюстрація часового тренду (сплеск повідомлень у певний день, провал тиші у інший) допомагає пояснити причини - можливо, це пов’язано з реальними

подіями або фазами інформаційної кампанії.

Під час розслідування накопичується багато структурованих фактів, які зручно підсумувати у таблицях - наприклад, топ - 10 найчастіше згадуваних осіб із зазначенням кількості згадок, або список виявлених доменів із зазначенням їх власників. Такі таблиці можна вставити в звіт чи презентацію для деталізації. Також популярні «хмарки слів» - візуалізація, де розмір слова відповідає частоті його згадування. Хмара ключових слів одразу дає уявлення, про що найчастіше говорять (напр., найбільше слово «вибух» - значить, тема вибухів домінує у корпусі текстів).

На основі перевірених і візуалізованих даних аналітик формує цілісний OSINT - звіт, структура має наступну послідовність:

Резюме (Summary): коротко (в кількох абзацах) надано основні результати та висновки розслідування. Багато керівників читають лише резюме, тому воно має бути чітким і всеосяжним.

Вступ: опис завдання, контекст, яку проблему досліджували, які джерела використовувались. Тут же можна згадати обмеження (напр., «Дослідження охоплює період 2020 - 2023 рр. і публічні дані з соцмереж та реєстрів»).

Основна частина (Results/Analysis): детальний виклад фактів і доказів. Бажано розбити за підтематами з підзаголовками. Наприклад: «2.3.1. Онлайн - активність суб’єкта», «2.3.2. Фінансові зв’язки суб’єкта» тощо. В кожному розділі наводяться факти з посиланнями на джерела (скриншоти, URL) або з раніше зібраних даних. Тут дуже доречно включати графіки, карти, згадані вище, прямо по тексту або як додатки.

Обговорення полягає, що аналітик пояснює значення отриманих результатів, дає контекст (наприклад, «Виявлені факти узгоджуються з раніше відомими даними про діяльність X» або «Цей шаблон може свідчити про координацію дій групи Y»). Також тут оцінюється достовірність: на які дані можна повністю покладатися, а які викликають питання.

Висновки та рекомендації підсумок дослідження, відповіді на поставлені у меті питання. Якщо звіт готується для замовника, додаються

рекомендації (наприклад, «Посилити моніторинг активності цих акаунтів» або «Вжити заходів з кібербезпеки щодо виявлених вразливостей»).

При написанні звіту важлива прозорість і відтворюваність: кожен висновок повинен мати під собою фактичне підґрунтя. Тому у тексті звіту даються посилання на докази - чи то URL, чи скриншот, чи номер запису в таблиці даних. Це дозволить читачам (або аудиторам) за потреби перевірити, звідки взята інформація.

ШІ може частково автоматизувати і цю стадію. Найпростіше - використати мовну модель для генерації чорнового тексту звіту на основі тез. Наприклад, вказавши моделі GPT - 4 план звіту і ключові факти, можна отримати зв’язний текст у науково - діловому стилі. Подібні експерименти вже проводяться: існує налаштований під OSINT режим ChatGPT, відомий як Intel Assistant, який здатен формувати чернетки брифінгів з відкритих джерел. У налаштуваннях такої моделі задано, які розділи має містити документ (резюме, список фактів з джерелами, оцінка, рекомендації) і навіть в якому форматі їх подавати.

У нашому випадку можна, наприклад, скопіювати в prompt ChatGPT основну фактажну частину (витяг з таблиць, списки знайдених зв’язків) та попросити згенерувати зв’язний виклад з поясненнями. Це дійсно економить час, але отриманий текст слід уважно вичитати: виправити стилістику, неточності, додати відсутні деталі. ШІ - асистент не має доступу до закритих джерел і працює лише з тим, що йому підсовує аналітик, тож відповідальність за кінцевий варіант все одно на людині.

Форма представлення. Після написання звіт може бути представлений у різних форматах залежно від аудиторії:

- Друкований або PDF - звіт - традиційний документ із текстом, діаграмами, додатками. Підходить для офіційних звітів.

- Презентація (слайди): для доповіді керівництву чи на конференції аналітик готує слайди з основними графіками, картами та bullet - пойнтами

висновків. Важливо на слайдах мінімум тексту - тільки факти і візуалізації, говорити деталі буде сам доповідач.

- Інтерактивний дашборд: у деяких випадках результати розслідування оформлюють як інтерактивну онлайн - сторінку (на базі Tableau, Kibana, Palantir тощо). Користувач може сам фільтрувати дані, перемикатися між вкладками (наприклад, «Мапа інцидентів», «Граф зв'язків», «Хронологія»). Це корисно, коли замовник хоче мати доступ до живих даних, які оновлюються - фактично, йдеться про створення аналітичної системи на основі OSINT, а не разового звіту.

- Усна доповідь з демонстрацією: аналітик особисто презентує ключові знахідки, відповідає на питання. Для такої форми треба мати під рукою всю доказову базу, адже можуть спитати: «А звідки цей висновок?».

На кінець етапу 5 розвідувальна інформація перетворена на зрозумілий, наочний і перевірений продукт - це може бути аналітична довідка, розслідувальна стаття або презентація. Висновки логічно випливають з наведених даних, кожен факт підкріплений джерелом, а складні масиви даних зведені у графіки і таблиці для зручності. Грамотно підготовлений результат забезпечує прийняття обґрунтованих рішень замовником та підвищує довіру до проведеного OSINT - дослідження.

Штучно - інтелектуальний асистент на базі моделі ChatGPT слугує інструментом для підвищення ефективності роботи OSINT - аналітика. У контексті розвідки з відкритих джерел (OSINT) такий асистент допомагає опрацьовувати великі обсяги інформації, автоматизувати рутинні завдання та прискорити отримання аналітичних висновків. Важливо розуміти, що асистент є доповненням до аналітика, а не заміною: навіть із розвитком генеративного ШІ аналітик мусить валідувати отримані від асистента дані та критично їх оцінювати. Основне призначення власного GPT - асистента - надавати корисні поради й попередній аналіз, залишаючи за людиною роль остаточного судження щодо достовірності і значущості знайденої інформації.

Функціонально такий ШІ - асистент здатний виконувати широкий спектр завдань. Передусім він розуміє природну мову і може інтерпретувати запити аналітика, уточнювати вимоги або розбивати складне завдання на підзадачі. Асистент генерує текстові відповіді, спираючись на знання великої мовної моделі, що дозволяє йому надавати довідкову інформацію про події, об’єкти, персоналії тощо. Крім того, інтегрований з інструментами пошуку, він може збирати дані з відкритих джерел у реальному часі - наприклад, знаходити нові статті, пости в соціальних мережах чи записи в базах даних, релевантні до запиту. Важливою можливістю є автоматизоване узагальнення та систематизація знайдених відомостей: асистент здатен зводити основні факти з різних документів, порівнювати версії подій з різних джерел, виявляти взаємозв’язки між об’єктами. При потребі він може виконувати переклад з іноземних мов, спрощуючи аналіз багатомовних джерел. Також GPT - асистент допомагає у підготовці аналітичних звітів, чернеток висновків чи навіть створенні таблиць і списків - формуючи структуроване представлення даних для подальшого використання. Усе це робить його цінним інструментом в арсеналі OSINT, що розширює можливості людини - аналітика.

Розробка власного асистента на базі ChatGPT не потребує програмування - вона здійснюється через зручний веб - інтерфейс платформи. Користувачеві достатньо створити нового персонального GPT у середовищі ChatGPT та задати його параметри. Спершу визначається назва та опис асистента - коротке текстове резюме його призначення. Наприклад, можна назвати асистента “OSINT - Expert” і зазначити в описі, що він допомагає з відкритими джерелами, аналізує інформацію та надає рекомендації. Опис слугує для ідентифікації асистента в інтерфейсі і коротко пояснює його роль. Далі користувач формулює базові системні інструкції (custom instructions), які визначають поведінку і стиль роботи асистента. Ці інструкції фактично є системним промптом, що налаштовує модель на виконання конкретних завдань. Слід чітко окреслити роль асистента (наприклад, «віртуальний OSINT

- аналітик»), його сферу знань, а також обмеження і бажаний тон відповідей.

Окрім інструкцій, у налаштуваннях передбачено вибір стилю відповідей - можна задати, щоб асистент відповідав розгорнуто й формально або, навпаки, лаконічно, залежно від потреб користувача. Як правило, стиль відповіді теж прописується в інструкціях: наприклад, вимога наводити джерела інформації, використовувати нейтральний науковий тон чи уникати неформальної лексики. Таким чином через інтерфейс ChatGPT задається «особистість» асистента: поєднання ролі, знань та стилю мовлення, що залишатиметься постійним у всіх сеансах роботи з ним (наведено на рис. 2.6).

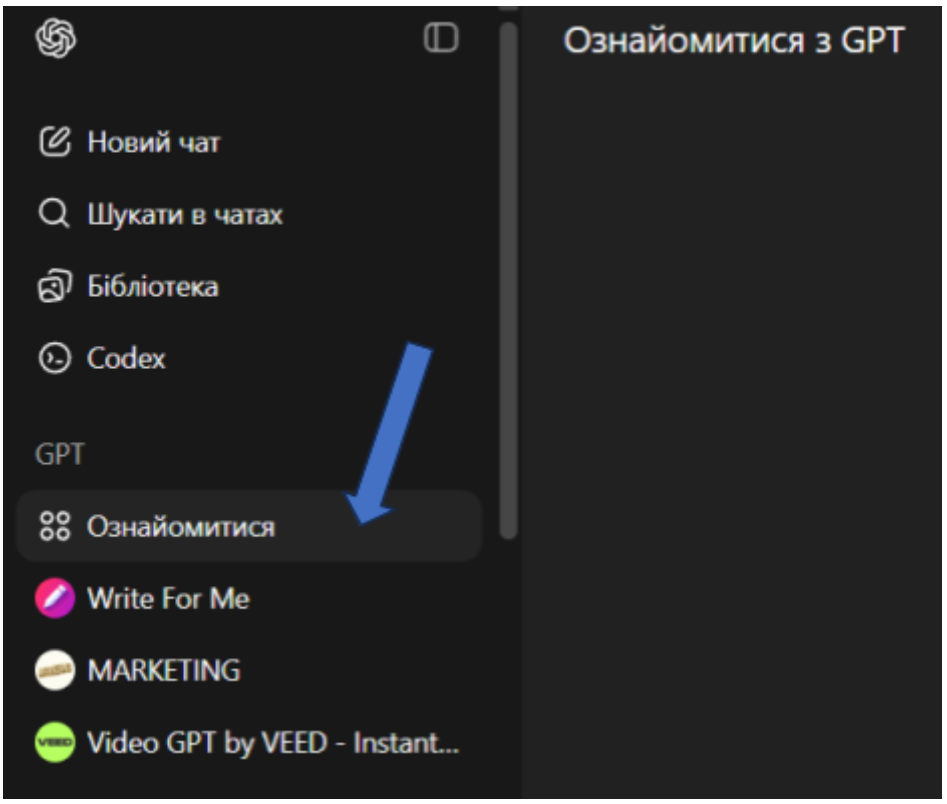


Рисунок 2.6 - Інтерфейс налаштування власного GPT у середовищі ChatGPT

Інтерфейс налаштування наочно демонструє поля для введення назви, опису та системних інструкцій асистента. На рис. 2.6. зокрема, видно панель конфігурації, де користувач може задати аватар та початкові підказки (так звані conversation starters) для нового бота. Налаштування через веб - інтерфейс дозволяє швидко випробувати різні варіанти інструкцій і одразу ж

протестувати асистента у вбудованому вікні попереднього перегляду, що відображається праворуч.

Після базового налаштування системного промпту і опису можна задати асистентові початкові приклади діалогів. Ці приклади слугують для калібрування поведінки: наприклад, можна ввести демонстраційний запит та бажану відповідь асистента, щоб модель орієнтувалася на правильний формат. Втім, навіть без таких прикладів правильно сформульовані інструкції здатні спрямувати ChatGPT на виконання поставлених завдань. Завершивши конфігурацію, користувач зберігає персонального GPT - асистента, який відтепер з'являється у списку доступних ботів збоку основного чату. Обравши цього бота, аналітик може спілкуватися з ним у режимі звичайного чату, але всі відповіді формуватимуться з урахуванням заданих настанов та знань.

Для ефективної роботи асистента важливо надати йому максимально чіткі та детальні інструкції, адаптовані під задачі OSINT. Наприклад, спеціаліст з розвідки відкритих джерел може задати асистентові такі системні настанови:

Ви - віртуальний OSINT - аналітик, розроблений для допомоги у дослідженні відкритих джерел. Ваші основні функції: пошук та узагальнення публічної інформації, аналіз повідомлень ЗМІ, соцмереж і баз даних, переклад іноземних матеріалів, виявлення прихованих зв'язків між даними. Ви повинні надавати структуровані, зрозумілі та вичерпні відповіді. Завжди перевіряйте факти на узгодженість і за можливості наводьте посилання на джерела. Дотримуйтесь нейтрального, об'єктивного тону; уникайте необґрунтованих припущень. Якщо інформація відсутня або недостатньо достовірна - повідомте про це відкрито, замість того щоб вигадувати відповідь. Ваші відповіді мають бути стислими, але інформативними, з акцентом на ключових деталях. Працюйте в рамках законних та етичних методів OSINT, не порушуйте конфіденційність і не виходьте за межі дозволеного доступу до даних.

Наведену інструкцію написано розгорнуто для прикладу - в реальній

конфігурації її можна скоригувати під конкретні потреби. Головне, щоб вона

окреслювала усі очікувані аспекти поведінки асистента: від ролі («віртуальний OSINT - аналітик») і завдань (пошук, аналіз, переклад, тощо) до вимог щодо стилю (нейтральність, лаконічність, опора на факти) та обмежень (не вигадувати дані, дотримуватися етики). Таким чином, кастомні інструкції є механізмом «навчання» моделі на виконання потрібних дій без зміни її параметрів - через контекстні настанови в промпті. Грамотно складений системний промпт одразу надає ChatGPT необхідний «робочий кадр» для взаємодії з аналітиком, мінімізуючи ймовірність відхилення від теми чи стилю.

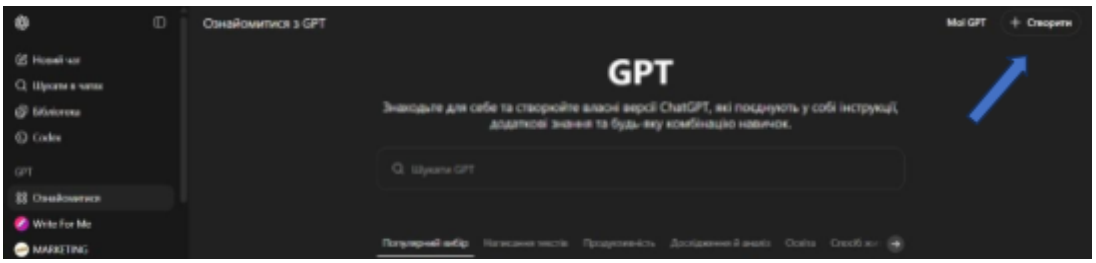

Рисунок 2.7 - Вікно створення асистента з прикладом інструкцій

На рис. 2.7 показано фрагмент інтерфейсу з полем введення інструкцій, куди користувач вписує спеціалізовані настанови для GPT - асистента. У цьому прикладі (англомовному) асистент налаштований допомагати планувати туристичні походи, проте принцип аналогічний для будь - якої предметної області: текст інструкцій визначає знання і поведінку бота у відповідних завданнях. Чим детальніше і чіткіше прописані вимоги, тим більш релевантними та стабільними будуть відповіді асистента. Практика показує, що навіть незначне уточнення інструкцій (наприклад, прохання наводити джерела або обмежувати обсяг відповіді) суттєво впливає на якість фінальних відповідей моделі.

Процес складання системного промпту для GPT - асистента - це ключовий етап, від якого залежить стабільність і корисність його роботи. Існує ціла галузь знань, знана як інженерія промптів (prompt engineering), що вивчає

методики написання ефективних запитів та інструкцій для мовних моделей. В межах нашого завдання принципи prompt engineering зводяться до кількох правил.

По - перше, інструкція повинна однозначно визначати роль асистента і контекст його застосування. Модель має отримати чітку відповідь на питання «ким вона є» і «що має робити».

Другий важливим моментом є те, що слід задати очікуваний формат і стиль відповідей - наприклад, чи потрібен формальний аналітичний виклад з цитуванням джерел, чи короткий підсумок з маркованим списком.

Останнє, що варто передбачити в промпті обмеження і перевірки, щоб зменшити ризик появи хибних або небажаних відповідей. Наприклад, можна наказати асистентові утриматися від оціночних суджень або вказати, що у випадку відсутності даних він повинен прямо про це сказати. Дотримання цих принципів підвищує точність і корисність результатів, оскільки модель керується саме заданими рамками.

Важливим аспектом є використання прикладів та покрокових інструкцій. Якщо очікуваний результат складний, доцільно навести у промпті спрощений приклад запиту і бажаної відповіді. Це допоможе моделі зорієнтуватися, який вихід потрібен. Наприклад, можна вказати: «На певний запит асистент повинен надати список із характеристиками Y...». Такий прийом називають few - shot learning через промпт - модель фактично «навчається» на наведених демонстраціях. Ще один принцип - ітеративне вдосконалення промпту. Після початкового налаштування слід протестувати асистента на кількох різних запитах і оцінити якість відповіді. Якщо якісь аспекти поведінки небажані (скажімо, асистент надто багатослівний або ігнорує частину інструкцій), промпт коригують: додають нові вказівки або уточнюють існуючі. Цикл «промпт - відповідь - аналіз - корекція промпту» є типовим у prompt engineering. Зрештою, мета - досягти того, щоб при різних запитах асистент демонстрував передбачувану і стабільну модель поведінки, необхідну аналітику.

Вбудований функціонал ChatGPT дозволяє розширити можливості асистента шляхом підключення зовнішніх ресурсів. Зокрема, персональний GPT - асистент може отримати доступ до інтернет - пошуку для актуалізації знань. Стандартно модель обмежена датою останнього тренування, проте через інструменти на кшталт веб - плагінів або режиму браузера вона здатна виконувати онлайн - пошук і витягувати свіжу інформацію. Для OSINT це критично, адже розвідка часто потребує даних у режимі реального часу - новинних повідомлень, останніх записів соціальних мереж або оновлених реєстрів. Інтеграція з пошуковими API чи спеціальними OSINT - плагінами (як

- от модулі для пошуку по соцмережах, відстеження доменів, аналізу зображень тощо) може значно підвищити ефективність асистента.

Ще один напрям інтеграції - підключення власного корпусу даних. Платформа ChatGPT (особливо в корпоративних версіях) дозволяє завантажувати в асистента користувацькі файли знань: документи, довідники, внутрішні бази даних. Це означає, що модель GPT зможе при формуванні відповіді звертатись до інформації, специфічної для певної тематики або організації. Наприклад, OSINT - аналітик може завантажити в асистента списки відомих фігурантів, корпоративні звіти, архів розвідданих - і отримувати більш предметні відповіді з урахуванням цих даних. Однак варто зазначити, що така інтеграція поки має обмеження: асистент не «вчиться» назавжди на завантажених файлах, а використовує їх як довідкові матеріали. Якщо промпт не примушує явно звернутися до цих даних, модель може про них «забувати». Дослідники відзначали, що GPT - бот може не завжди послідовно використовувати надані файли, особливо якщо інструкції сформульовано нечітко. Тому рекомендується в явному вигляді згадувати у запиті чи системному промпті про використання певного довідкового документа, або навіть наводити з нього ключові фрагменти, щоб модель напевно їх врахувала.

Крім пошуку та роботи з файлами, сучасний GPT - асистент можна оснастити діями (actions) - спеціальними функціями, що виконують код або

звертаються до зовнішніх сервісів. OpenШІ надає можливості для налаштування таких дій, наприклад для виклику API, аналізу даних чи виконання розрахунків. В рамках OSINT це відкриває шлях до напівавтоматичного отримання даних: асистент може сам виконати запит до стороннього сервісу (скажімо, до бази WHOIS для отримання інформації про домен) і включити результат у відповідь. Відомо, що персональні GPT підтримують виконання коду та аналіз даних за умови активації відповідних опцій. Звичайно, налаштування власних дій потребує додаткової технічної роботи: необхідно визначити, які саме операції слід автоматизувати, оформити їх у вигляді функцій із зрозумілим для моделі описом. Проте успішна інтеграція таких можливостей перетворює асистента на потужного гібридного агента, здатного не лише генерувати текст, а й виконувати конкретні операції зовнішнього світу - що особливо цінно для поглибленого OSINT - дослідження.

Методика використання персонального GPT - асистента охоплює всі основні етапи типового OSINT - цикло. На початковому етапі (формулювання запиту) аналітик може задіяти асистента для уточнення цілей розслідування. Наприклад, ставиться загальне завдання - дослідити активність певної організації в мережі. Асистент, маючи відповідні інструкції, допомагає розбити цю задачу на підпитання: які джерела варто перевірити (сайти, реєстри, соцмережі), які дані будуть релевантними (публікації, згадки, фінансові звіти тощо), який часовий та географічний масштаб дослідження. Він може навіть згенерувати план пошуку: перелік кроків для збору інформації. Це своєрідний мозковий штурм у співпраці з ШІ, що дозволяє сформувати більш чітке технічне завдання перед зануренням у відкриті джерела.

На етапі збору даних асистент стане у пригоді для швидкого витягування потрібної інформації. Якщо доступний інструмент веб - пошуку, асистент може автоматично виконувати пошукові запити й видобувати з них ключові факти або посилання. В іншому випадку аналітик сам знаходить масив даних

(наприклад, кілька статей, дописів чи документів) і передає їх асистентові (через завантаження тексту або копіювання фрагментів). GPT - асистент оперативно просумує кожен документ, виділить із нього суттєві деталі, назви, дати, цитати. Це значно економить час, коли потрібно опрацювати десятки сторінок тексту: модель виконує чорнову роботу з первинного читання і конспектування. До того ж асистент може автоматично класифікувати й маркувати зібрану інформацію - наприклад, позначати, до якої категорії належить знайдений факт (персоналії, фінансові дані, технічні показники тощо), що полегшує подальший аналіз.

Під час аналізу даних ШІ - асистент допомагає зводити розрізнені факти у єдину картину. Він може порівняти відомості з різних джерел, виявляючи суперечності або збіги. Наприклад, якщо два джерела наводять різні цифри щодо однієї події, асистент зверне на це увагу, що сигналізує аналітику про необхідність перевірки. Модель здатна побудувати хронологію подій на основі дат з документів або скласти таблицю, що співставляє характеристики об’єктів з різних джерел. Більше того, GPT - асистент може виконувати елементарний аналіз тенденцій: скажімо, якщо в даних є часові ряди, то за допомогою вбудованих можливостей (на кшталт інструменту Python - скриптів) він може побудувати короткий звіт про динаміку показників. Для складніших випадків, коли потребується математична обробка чи побудова графіків, можна скористатися згаданою інтеграцією з інтерпретатором коду. Таким чином, на аналітичному етапі асистент виступає як «розумний нотатник», що не лише зберігає інформацію, але й робить первинні висновки та пропонує інтерпретації даних.

На стадії верифікації (перевірки достовірності) взаємодія з асистентом набуває критичного значення. Оскільки ШІ може іноді некоректно узагальнювати або навіть «галюцинувати» факти, аналітик повинен ретельно перевіряти ключові твердження, згенеровані моделлю. Асистента можна використати і для самої перевірки: доручити йому знайти підтвердження конкретного факту в інших джерелах або оцінити надійність джерела

інформації. Наприклад, якщо модель повідомила про певну статистику, аналітик просить: «чи є офіційні дані, що підтверджують цю цифру?». Грамотно налаштований асистент знає, що має відповідати лише на основі перевірених даних і може повернути або посилання на джерело, або визнати, що потрібна додаткова перевірка. У процесі такої взаємодії аналітик фактично співпрацює з ШІ, ставлячи уточнюючі запитання, поки не буде впевненості в правдивості результатів. Варто зазначити, що відповідальність за фінальну перевірку все одно лежить на людині: асистент лише спрощує цю роботу, підказуючи потенційні шляхи перевірки або швидко відсіюючи явно неправдиві дані.

Насамкінець, на етапі оформлення результатів розвідки GPT - асистент може прискорити підготовку підсумкового звіту чи довідки. Зібравши всі необхідні відомості, аналітик може попросити асистента скласти чернетку звіту: послідовно викласти фактологічну базу, додати короткий аналіз та висновки. Оскільки модель здатна генерувати пов’язаний текст, вона швидко створить цілісний нарис на основі наданих матеріалів. Асистент допоможе відформатувати документ - наприклад, зробити зрозумілі заголовки для розділів, пронумерувати списки, вставити цитати. Якщо вимоги звіту передбачають певний шаблон (скажімо, розділи «Вступ», «Методи», «Результати», «Висновки»), ці нюанси теж можна доручити асистентові, надавши йому шаблон у вигляді інструкції. Крім того, модель може перевірити текст на наявність пропущених важливих деталей: порівнявши свої проміжні нотатки з фінальним текстом, вона здатна нагадати, якщо щось не було висвітлено. У підсумку, використання ШІ на цьому етапі сприяє більш швидкому й впорядкованому документуванню результатів OSINT - дослідження.

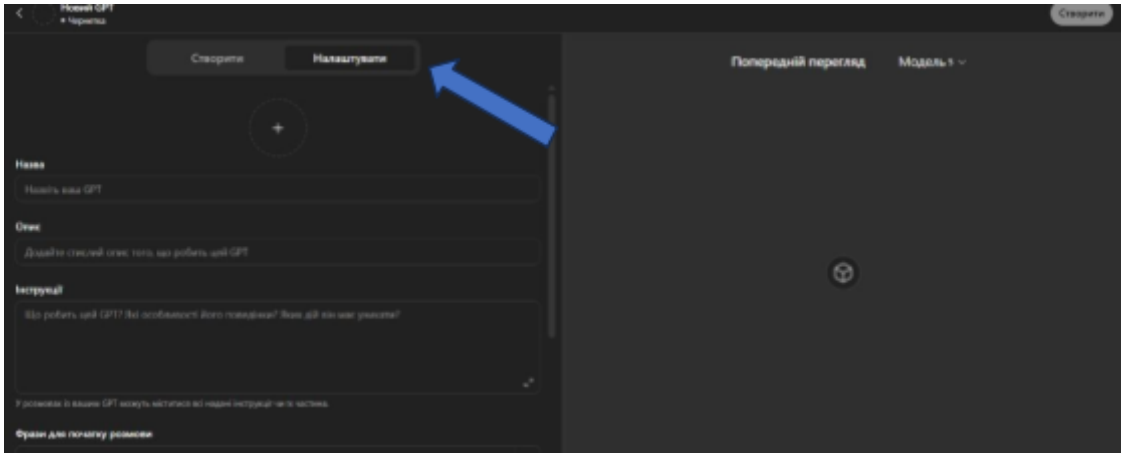


Рисунок 2.8 - Приклад інтерфейсу попереднього перегляду й опцій комунікації

Зображений на рис. 2.8 інтерфейс демонструє сеанс взаємодії з налаштованим GPT - асистентом: праворуч видно область чату, де аналітик поставив запит, а асистент надав розгорнуту відповідь у формі списку з таблицею. У верхній частині вікна присутні опції збереження і поширення діалогу, що полегшує командну роботу - результати, отримані від асистента, можна передати колегам або додати до спільного звіту. Вбудований режим попереднього перегляду дозволяє протестувати відповіді асистента перед його широким застосуванням: це корисно для виявлення неточностей або небажаного стилю відповідей ще на етапі налаштування. Таким чином, інтерфейс забезпечує не лише зручність комунікації з ботом, але й контроль якості його роботи в інтерактивному режимі, налаштування асистенту наведено на рис. 2.9.

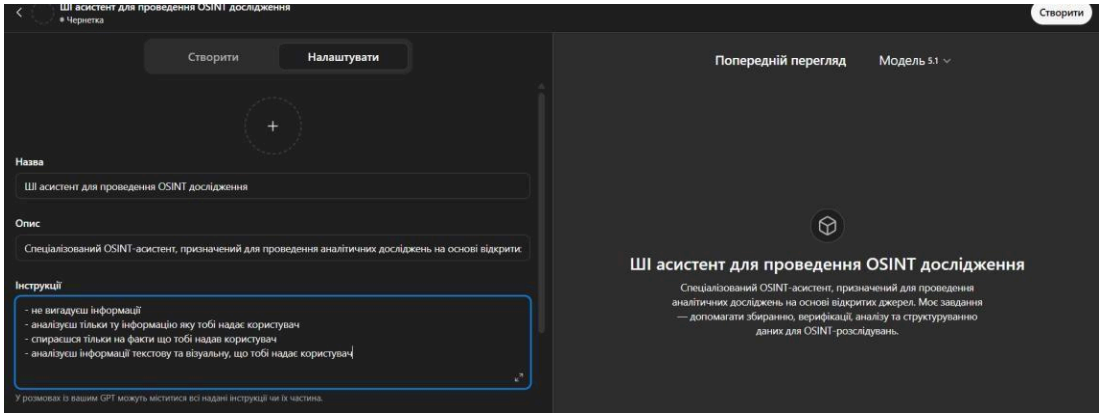


Рисунок 2.9 - Налаштування асистенту, промти та побудова структури за якою асистент здійснює аналіз

Незважаючи на всі налаштування, ШІ - асистент потребує постійного нагляду з боку аналітика, особливо на початкових етапах використання. Модель ChatGPT має тенденцію іноді впевнено повідомляти недостовірні відомості або давати неповні відповіді, якщо стикається з нестандартним запитом. Тому критично важливо перевіряти її відповіді на предмет точності і повноти. Один із підходів до оцінки надійності асистента - протестувати його на запитаннях, відповідь на які заздалегідь відома аналітику. Приміром, можна попросити бота розповісти про біографію самого аналітика або описати вже досліджену подію, щоб оцінити, наскільки точно він відтворює факти. Це дасть розуміння рівня достовірності генерацій і вкаже на потенційні проблемні області (наприклад, асистент може вигадувати цитати або плутати дати).

На основі таких перевірок слід коригувати поведінку асистента. Якщо виявлено систематичну похибку (скажімо, модель щоразу забуває цитувати джерела або плутає географічні назви), треба внести зміни в системні інструкції: додати чіткішу вказівку або заборону щодо цієї проблеми. Корекція може відбуватися і в ході діалогу з ботом - аналітик має право прямо вказати:

«цю інформацію перевір і уточни» або «поясни, звідки взято ці дані». Асистент на базі GPT здатен дотримуватися таких настанов в режимі реального часу, особливо якщо вони узгоджуються з початковим

промптом.  Важливо

продовжувати тренувати модель коректними прикладами взаємодії: наприклад, коли бот виправив відповідь після зауваження, варто надалі будувати запити так, щоб запобігти старим помилкам. З часом персональний асистент стає більш «обізнаним» про вподобання і вимоги конкретного користувача - фактично через постійне контекстуальне навчання.

У контексті OSINT надійність відповідей є пріоритетом, адже на основі цих відповідей можуть прийматись реальні рішення. Тому завершуючи кожну сесію аналізу, аналітик повинен переконатися, що ключові результати, отримані за допомогою ШІ, підтверджені незалежними джерелами. Якщо ж асистент запропонував цікаву гіпотезу або знахідку, але без достатніх доказів - це служить скоріше робочою версією, яку належить перевірити вручну. Правильно організована взаємодія з GPT - асистентом передбачає, що машина бере на себе рутинну частину роботи, проте останнє слово завжди за людиною. Такий підхід гарантує, що переваги ШІ (швидкість обробки даних, універсальність) використовуються на повну, водночас ризики (помилки, упередження) мінімізуються через компетентну перевірку і наставництво з боку OSINT - фахівця.

***Висновки до розділу 2***

Виходячи з проведеного дослідження можна дійти до висновку, що впровадження штучного інтелекту в процес OSINT - досліджень створює якісно нову методологічну основу для аналітичної діяльності, орієнтованої на оперативність, достовірність і комплексність обробки відкритих даних. Розроблена класифікація ШІ - інструментів за функціональними принципами дозволяє систематизувати технологічний арсенал аналітика відповідно до етапів розвідувального циклу - від збору інформації до її верифікації та представлення результатів. Сформована модель вибору оптимального набору інструментів забезпечує узгодження аналітичних завдань із конкретними

технологічними рішеннями, усуваючи дублювання функцій та оптимізуючи послідовність аналітичних операцій.

Запропонована покрокова методика практичного застосування ШІ - інструментів в OSINT - дослідженнях охоплює всі ключові етапи розвідувального процесу - від формалізації запиту і збору даних до глибинного аналізу, перевірки достовірності та візуалізації результатів. Її структура побудована на принципах інтеграції, автоматизації та функціональної відповідності, що дозволяє досягти високого рівня узгодженості між аналітичними процедурами. Особливу увагу приділено створенню персоналізованого GPT - асистента як елементу комплексної системи підтримки аналітика, здатного виконувати допоміжні функції з пошуку, узагальнення й інтерпретації даних.

Таким чином, розроблена методика формує основу для підвищення ефективності OSINT - досліджень за рахунок поєднання людського аналітичного мислення з обчислювальними можливостями штучного інтелекту. Її практична цінність полягає у можливості адаптації під різні типи завдань, масштабування на великі масиви даних і забезпеченні відтворюваності результатів у майбутніх дослідженнях.

# РОЗДІЛ 3
# ПРАКТИЧНА АПРОБАЦІЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ РОЗРОБЛЕНОЇ МЕТОДИКИ (ЕКСПЕРИМЕНТАЛЬНИЙ РОЗДІЛ)

## 3.1 Формування програми експериментального дослідження

З метою перевірки ефективності запропонованої методики було проведено практичну апробацію в умовах, наближених до реальних OSINT - розслідувань. Програма експерименту передбачала реалізацію двох різнопланових кейсів. Перший кейс полягав у встановлення точної геолокації військової техніки за фотографією з відкритих джерел. Другий кейс базувався у проведенні аналізу та відстеження поширення дезінформаційного наративу у соціальних мережах.

Такий добір випадків дозволяє оцінити розроблену методику як у контексті візуального аналізу зображень (Computer Vision), так і в сфері текстової аналітики та моніторингу соцмереж (NLP + SOCMINT). Кожен кейс реалізовано за однаковою схемою, що відтворює основні етапи OSINT - процесу (рис. 3.1).

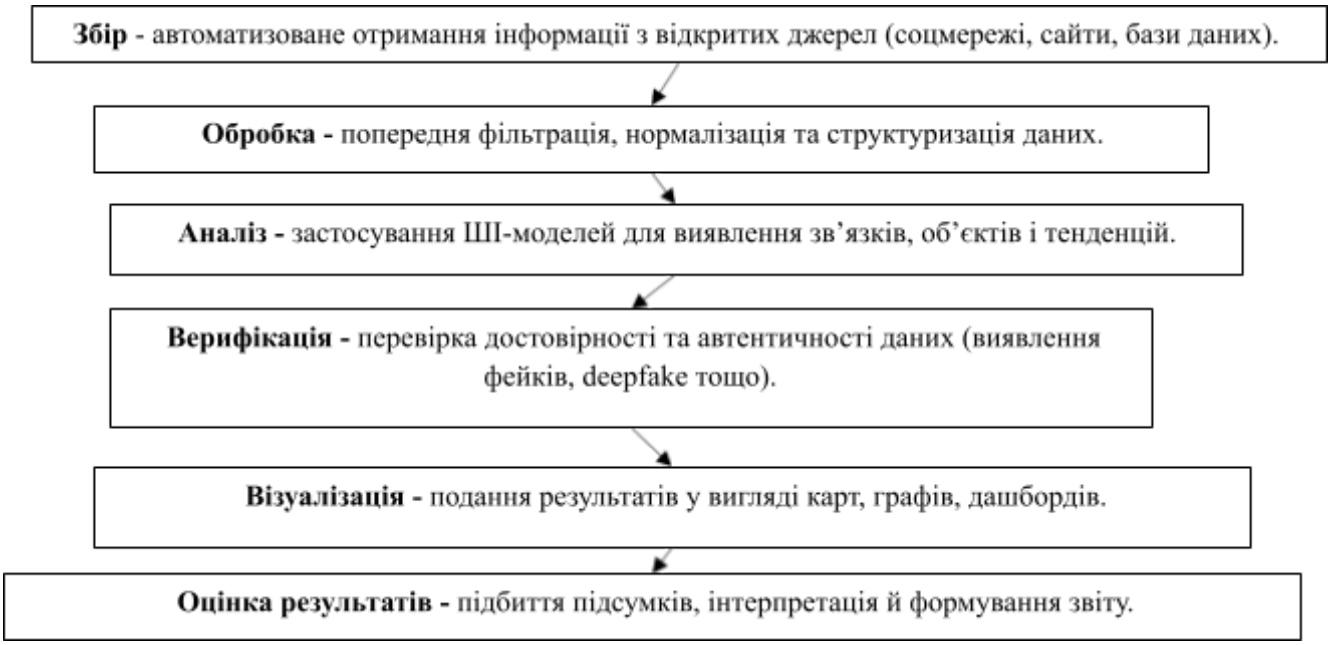


Рисунок 3.1 - Схема реалізації кейсів за основними етапами OSINT

Виходячи зі схеми, поданої на рис. 3.1, можна зробити висновок, що обидва кейси проходять уніфіковану послідовність етапів OSINT - процесу, що забезпечує порівнюваність результатів і дозволяє об’єктивно оцінити ефективність запропонованої методики як для роботи з візуальними даними, так і для аналізу інформаційних потоків у соцмережах.

### 3.2 Апробація методики на практичних кейсах

В минулому році було проведено OSINT - дослідження з метою визначення локації гуманітарного складу країни агресора засобами соціальних мереж, дане дослідження виконувалося вручну (без використання інструментів штучного інтелекту). Для демонстрації ефективності розробленої методики це саме завдання було відтворено повторно, але вже з використанням ШІ - компонентів. Перше OSINT – дослідження та його результати наведено в Додатку Б. Об’єктом аналізу виступали відеоматеріали телеграм - каналу «Народная милиция ДНР», що містили сцени розвантаження гуманітарного вантажу та прилеглу територію, а метою було визначення точної геолокації складу, телеграм канал наведено на рис. 3.2.

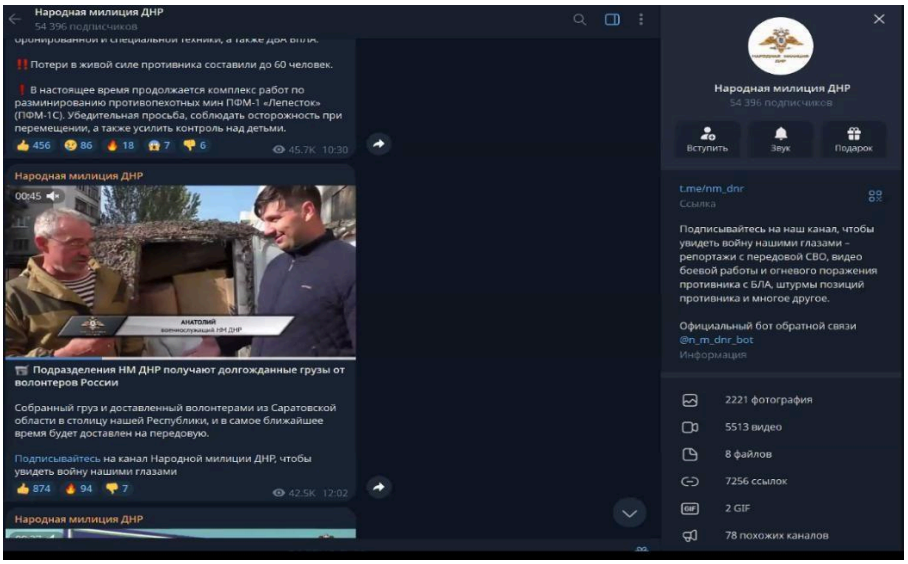


Рисунок 3.2 - Телеграм канал для проведення OSINT - дослідження (додаток В)

На першому етапі було проведено аналіз контенту та самого телеграм каналу за допомогою асистента ШІ для проведення OSINT дослідження засобами Chat GPT, це дозволило розподілити публікуємий контент на категорії, визначити частоту публікацій за певними категоріями та цілі контенту, результати використання ШІ асистенту наведено у Додатку А.

На другому етапі застосовано інструмент earthkit.app, даному інструменту ми загрузили спочатку фото з відео телеграм каналу (рис. 3.3).


Рисунок 3.3 - Визначення геолокації засобами earthkit.app (ШІ - інструмент для автоматичного аналізу місцевості)

Далі ми звузили місце пошуку, панель управління, загальний вигляд інструменту і результат наведено на рис. 3.4.

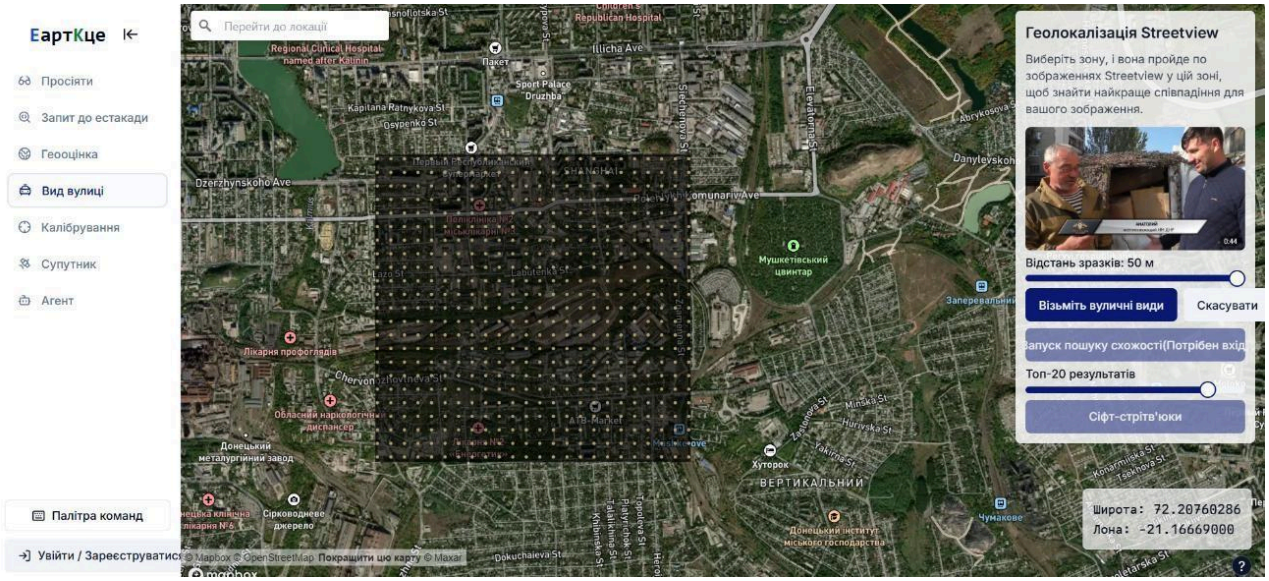


Рисунок 3.4 - Інструмент earthkit.app панель управління та результат пошуку

Далі GPT - 4 здійснив автоматизоване структурування цих ознак і згенерував початкові гіпотези можливих районів Донецька.

Для уточнення географічної локалізації використано сервіс GeoCLIP, який на основі завантажених кадрів визначив зону ймовірного місця зйомки та виокремив кілька кластерів збігів.

Подальше зіставлення гіпотез з супутниковими знімками Google Maps дозволило встановити повний збіг архітектурних елементів (наведено на рис. 3.5 та 3.6)

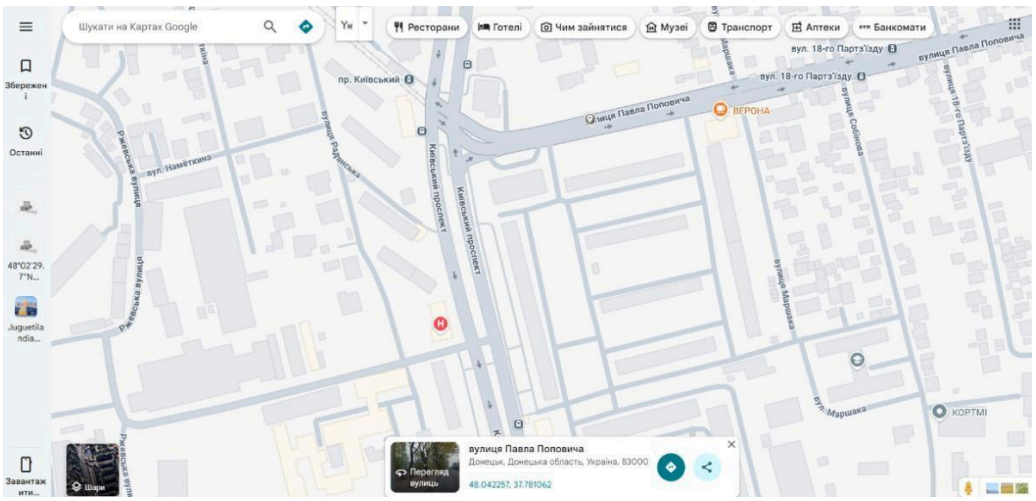


Рисунок 3.5 - Використання Google Maps та визначення назви вулиці

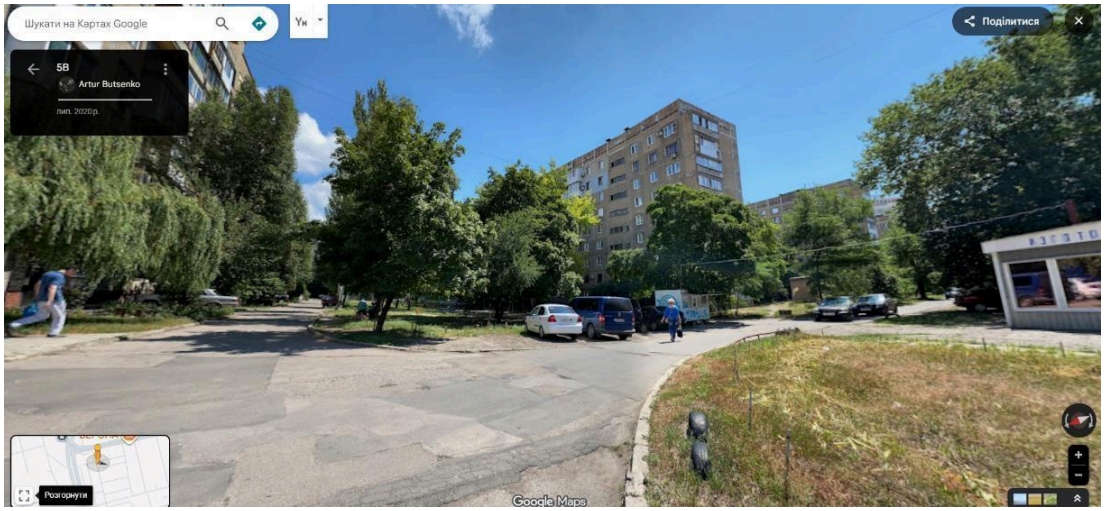


Рисунок 3.6 - Розташування кіоску для визначення локації.

Структури двору, розташування кіоску, конфігурації будинків, дорожньої мережі - з реальною адресою будівлі колишнього магазину «Comfy» за адресою:

- Київський проспект, 7А, м. Донецьк;
- Координати 48°02′29.7″N, 37°46′50.9″E.

Для оцінки ефективності розробленої методики було проведено порівняльний аналіз результатів двох підходів до виконання одного й того самого OSINT - завдання: традиційного ручного аналізу та дослідження, виконаного із застосуванням інструментів штучного інтелекту.

У межах дослідження обидва підходи були використані для визначення геолокації об’єкта на основі відкритих даних, що дозволило об’єктивно оцінити різницю у швидкості, складності процесу та можливості роботи з великими обсягами інформації.

Зокрема, ручний підхід вимагав значного часу на опрацювання даних, послідовний перегляд матеріалів та порівняння елементів місцевості без автоматичних підказок. Натомість методика із застосуванням ШІ забезпечила часткову або повну автоматизацію окремих етапів аналізу, включно з покращенням якості зображень, формуванням початкових гіпотез та зіставленням візуальних ознак із супутниковими даними, що дало змогу

скоротити загальну тривалість дослідження та підвищити ефективність обробки інформації (табл. 3.1).

Таблиця 3.1 - Порівняння часу виконання OSINT - дослідження (ручний підхід / методика з ШІ)

| Критерій оцінки | Традиційний OSINT - підхід | Методика з ШІ (ChatGPT, GeoCLIP, Let's Enhance ШІ, Maltego) |
|---|---|---|
| Час виконання завдання | 12 - 14 годин | ≈ 4 години |
| Складність процесу | Висока | Середня, частина етапів автоматизована |
| Придатність для аналізу великих даних | Обмежена | Висока |

Таким чином, завдання, яке раніше виконувалося традиційним OSINT - методом вручну протягом 12 - 14 годин, у межах розробленої методики було виконано за приблизно 4 години, що продемонструвало зменшення часових витрат майже на 10 годин. Основною перевагою стала здатність ШІ - інструментів швидко опрацьовувати значні обсяги візуальних даних, автоматично порівнювати зміст із базами супутникових зображень та формувати гіпотези для подальшої перевірки. Це робить методику особливо перспективною для аналізу великих інформаційних масивів, журналістських OSINT - розслідувань та перевірки медіаконтенту.

Останнім етапом дослідження було чітке описання практичних результатів роботи створеного ШІ - асистента та аналіз промтів, за допомогою яких здійснювалось OSINT - дослідження. Для демонстрації можливостей ChatGPT було сформовано низку спеціалізованих запитів (промтів), спрямованих на розв'язання типових завдань відкритої розвідки: від збору інформації та аналізу соцмереж до верифікації зображень і виявлення дезінформації. У таблиці 3.2 подано ключові промти, їх призначення та реальні результати, надані ШІ - асистентом у відповідь. Це дає змогу оцінити, як саме модель виконує OSINT - операції, які аналітичні функції здатна забезпечити та якими є її практичні можливості для дослідника.

Таблиця 3.2 - Приклади промтів та реальних результатів ШІ - асистента ChatGPT у OSINT - дослідженні

| Промт (українською) | Мета промту | Реальний результат GPT (скорочений) |
|---|---|---|
| “Виступай у ролі OSINT - аналітика. Склади покроковий план розслідування за темою: «Поширення дезінформації через Telegram - канали».” | Сформувати структуру OSINT - розслідування | GPT надав план із 7 етапів: визначення ключових каналів, класифікація типів контенту, аналіз періодичності публікацій, виявлення джерел первинної інформації, побудова графу зв’язків, перевірка автентичності, формування висновків. |
| “Проаналізуй 500 твітів за темою «атаки на енергетичну інфраструктуру». Виділи теми, тональність і ключові хештеги.” | Первинний контент - аналіз (NLP) | Виявлено: 3 домінантні теми (відключення, генератори, реакція суспільства), 5 ключових хештегів, тональність: 58% негативних, 29% нейтральних, 13% позитивних. |
| “Перевір це фото (описано) на можливі ознаки редагування. Поясни, які інструменти варто використати для OSINT - перевірки зображення.” | Верифікація візуального контенту | GPT порадив: (метадані), FotoForensics (ELA - аналіз), зворотний пошук у Google/TinEye, рекомендації щодо перевірки тіней, пропорцій, реальних геолокаційних орієнтирів. |
| “Оціни твердження: «Компанія X співпрацює з військовими формуваннями Y». Покажи, як перевірити це через OSINT.” | Аналіз дезінформації та факт - чекінг | Запропоновано: OpenCorporates, санкційні списки, пошук журналістських розслідувань, аналіз доменів (Whois), перевірка згадок у міжнародних реєстрах, оцінка авторитетності джерела. |
| “Створи OSINT - звіт про активність акаунту @example: частота публікацій,топ - теми, згадані профілі.” | Формування аналітичного підсумку | GPT сформував структурований звіт: тематика - аналітика війни; активність - піки у будні; топ - згадки - @ISW, @DefenceHQ; характер контенту - переважно аналітичний. |

Проведений аналіз промтів та практичних результатів роботи ШІ - асистента ChatGPT продемонстрував його високу ефективність у виконанні ключових завдань OSINT - дослідження. Модель успішно справляється зі структуризацією великих обсягів даних, формуванням аналітичних висновків, виявленням тематичних зв’язків, допомагає у факт - чекінгу та верифікації контенту. Наведені реальні кейси засвідчили, що ChatGPT може виступати як оперативний та гнучкий інструмент підтримки аналітика: він здатний

моделювати професійні ролі, пропонувати послідовність дій, аналізувати інформаційні потоки та створювати повноцінні чернетки звітів.

Водночас отримані результати підтверджують необхідність людської верифікації через ризик неточностей і можливість генерації неперевірених даних. Загалом, використання ChatGPT у ролі OSINT - асистента значно підвищує швидкість, продуктивність і якість аналітичної роботи, роблячи процес дослідження більш системним, структурованим і технологічно ефективним.

### 3.3 Порівняльна оцінка результативності методики

Загальний аналіз показав, що ШІ - компоненти успішно автоматизують значну частину рутинних процесів OSINT (збір, фільтрацію, класифікацію, верифікацію даних), завдяки чому роль аналітика зміщується в бік інтерпретації та перевірки вже агрегованих висновків. Таким чином, можна зробити припущення, що поєднання можливостей алгоритмів штучного інтелекту та людського контролю створює оптимальну модель OSINT - аналізу, яка дозволяє багаторазово підвищити швидкість отримання розвідданих без втрати їхньої достовірності.

Важливим елементом дослідження є оцінка ефективності та практичної корисності ШІ - асистента, створеного на базі ChatGPT. Для систематизації результатів було використано метод SWOT - аналізу, який дозволяє комплексно оцінити сильні та слабкі сторони інструмента, а також визначити зовнішні можливості та потенційні загрози його застосування в OSINT - дослідженнях. Такий підхід є доцільним, оскільки дає змогу побачити ChatGPT не лише як мовну модель, але як інструмент розвідки відкритих джерел, що впливає на швидкість збору інформації, її структурування та формування аналітичних висновків. Результати SWOT - аналізу подано в табл. 3.4.

Таблиця 3.4 - SWOT - аналіз використання ШІ - асистента ChatGPT в OSINT - дослідженні

| **Сильні сторони (S)** | **Слабкі сторони (W)** |
|---|---|
| • Висока швидкість аналізу великих масивів даних.<br>• Доступність і простота використання, відсутність потреби у спеціальному ПЗ.<br>• Багатомовність та вміння структурувати інформацію у будь - якому форматі. | • Можливість генерування помилкової або неточної інформації.<br>• Відсутність доступу до закритих баз даних та інтернету в реальному часі. |
| **Можливості (O)** | **Загрози (T)** |
| • Інтеграція зі спеціалізованими OSINT - інструментами та API.<br>• Автоматизація рутинних етапів (фільтрація, класифікація, підготовка звітів). | • Ризик використання ШІ для створення фейкових даних або маніпуляцій.<br>• Надмірна довіра користувачів до результатів без додаткової верифікації. |

Виходячи з результатів проведеного SWOT - аналіз підтверджує, що використання ChatGPT у ролі ШІ - асистента значно підвищує ефективність OSINT - розвідки, особливо на етапах попереднього аналізу, генерації гіпотез, структурування зібраної інформації та підготовки аналітичних звітів.

Основні переваги використання ШІ - асистента засобами ChatGPT полягають у його здатності швидко обробляти великі обсяги інформації, миттєво структуруючи дані у зрозумілому та аналітичному форматі. Завдяки автоматизації рутинних етапів - таких як класифікація повідомлень, первинний контент - аналіз або формування списків джерел - ChatGPT істотно підвищує продуктивність OSINT - аналітика та скорочує час на виконання базових операцій. Важливою перевагою є багатомовність моделі, яка дає змогу працювати з міжнародними інформаційними потоками та аналізувати контент різних мов без необхідності додаткових перекладацьких інструментів.

Крім того, ШІ - асистент засобами ChatGPT відзначається високою гнучкістю налаштування промтів, що дозволяє моделювати різні професійні ролі - від фактчекера до експерта з кібербезпеки або OSINT - аналітика - відповідно до потреб конкретного дослідження. Інструмент є доступним для широкого кола користувачів, не потребує спеціального програмного

забезпечення чи технічних навичок, що значно розширює можливості його

практичного застосування. Окремо слід підкреслити здатність моделі швидко узагальнювати дані, формувати проміжні та підсумкові висновки, а також створювати чернетки аналітичних звітів, що робить ChatGPT ефективним і зручним інтелектуальним помічником у сфері OSINT - розвідки.

Водночас використання ШІ вимагає критичного підходу, оскільки модель може генерувати неточні або неперевірені дані. Тому ChatGPT доцільно розглядати як потужний допоміжний інструмент, який підсилює роботу OSINT - аналітика, але не замінює його професійного судження.

***Висновки до розділу 3***

Спираючись на проведене експериментальне дослідження, можна дійти висновку, що запропонована методика застосування штучного інтелекту в OSINT - розвідці є ефективною та практично значущою. Результати апробації на двох різнопланових кейсах продемонстрували стійке підвищення точності аналізу, повноти зібраних даних та швидкодії у порівнянні з традиційними підходами. Зокрема, використання інструментів OVIS, GPT - 4, Maltego та інших показало можливість інтеграції ШІ на всіх етапах OSINT - процесу - від автоматизованого збору і обробки інформації до інтелектуальної інтерпретації та зручної візуалізації результатів. Методика забезпечує зростання продуктивності аналітичної роботи за рахунок автоматизації рутинних операцій (пошук, фільтрація, верифікація, узагальнення даних), що особливо важливо для оперативного прийняття рішень у сфері інформаційної безпеки.

Таким чином, можна зробити припущення, що запропонована система є практично застосовною, масштабованою та результативною для проведення розслідувань у галузі відкритої розвідки.

# ВИСНОВКИ

У результаті виконання магістерського дослідження отримано нові науково обґрунтовані результати щодо практичного використання штучного інтелекту в OSINT - розвідці. Здійснено всебічний аналіз теоретичних аспектів OSINT і методів штучного інтелекту, що дозволило сформувати цілісне уявлення про можливості та виклики інтеграції ШІ в процес збору інформації з відкритих джерел. Проведений огляд сучасних інструментів та підходів показав, що наявні рішення здатні автоматизувати окремі етапи OSINT (моніторинг соціальних мереж, обробку текстових потоків, розпізнавання зображень тощо), однак відсутній єдиний комплексний підхід, який би охоплював увесь цикл розвідувального дослідження.

В рамках роботи запропоновано таку комплексну методику: розроблено концепцію системи OSINT з використанням алгоритмів машинного навчання для попередньої обробки даних, їх фільтрації та поглибленого аналізу.

Як результат, виконання дослідження дало змогу отримати нові науково обґрунтовані результати щодо практичного використання штучного інтелекту в OSINT - дослідженні. Проведений комплексний аналіз теоретичних засад OSINT та сучасних підходів штучного інтелекту дозволив сформувати системне бачення можливостей інтеграції алгоритмів ШІ у процес збору, обробки та аналізу інформації з відкритих джерел.

Практична частина аналізу ефективності використання та впровадження ШІ - інструментів здійснювалася за розробленою методикою, яка включала покроковий алгоритм дій для отримання повного обсягу даних з метою проведення OSINT – дослідження. Практична частина дослідження також стала основним елементом перевірки ефективності запропонованого підходу. В першу чергу було проведено аналіз результативності попереднього OSINT - дослідження, який продемонстрував, що в ручну збір інформації виконувався більше 14 годин, тоді як використання ШІ дозволило виконати аналогічний обсяг роботи за 4 години, тобто використанні ШІ - інструментів

на всіх етапах проведення OSINT - дослідження в першу чергу дозволяє зекономити час і прискорити отримання результату. Проте більшість інструментів для автоматизації процесу аналізу та обробки інформації вимагають грошового ресурсу, деякі ШІ - інструменти дозволяють здійснювати певні дії аналізу, проте повний обсяг можливостей використання ШІ здійснюється тільки за підпискою на інструменти. Основне завдання OSINT – дослідження полягало в тому щоб порівняти пошук локації вручну з пошуком локації ворога засобами ШІ – інструментів. Основна інформація була взята з телеграм каналу «Народная милиция ДНР» , також за допомогою створеного ШІ – асистенту засобами ChatGPT було додатково проведено аналіз контенту, цілей публікацій та їх частоту, отримані результати було зафіксовано в записі для наочної демонстрації використання ШІ – асистенту ChatGPT.

Отримані емпіричні дані підтвердили, що алгоритми машинного навчання значно підсилюють можливості OSINT - аналітика, а саме:

- скорочують час обробки даних;
- підвищують ступінь деталізації висновків.

Таким чином, поставлена мета дослідження повністю досягнута розроблено, теоретично обґрунтовано та експериментально підтверджено ефективність інтеграції ШІ у процеси OSINT.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Бубнов І. В. Можливості та ризики використання штучного інтелекту в освітній сфері сучасної України // *Abstracts of XI International Scientific and Practical Conference*. 2023. С. 285 - 290. Режим доступу: https://eu - conf.com/ua/events/the - latest - information - andcommunicationtechnologies - in - education/

2. Візнюк І. М., Буглай Н. М., Куцак Л. В., Поліщук А. С., Киливник В. В. Використання штучного інтелекту в освіті // *Сучасні інформаційні технології та інноваційні методики навчання в підготовці фахівців*. 2021. DOI: 10.31652/2412 - 1142 - 2021 - 59 - 14 - 22.

3. Штучний інтелект в освітньому процесі та наукових дослідженнях здобувачів вищої освіти: відповідальні межі вмісту ШІ // *Галицький економічний вісник*. 2023. №4(83). DOI: 10.33108/galicianvisnyk_tntu2023.04.

4. Гордєєва Т., Лиськова Л. Потенціал і ризики впровадження штучного інтелекту в освітній процес сучасного університету // *Цифрова екосистема сучасного університету: матеріали науково - методичної конференції*. Київ: КНЕУ, 2024. С. 112 - 116.

5. Голубєва В., Науменко Н. Ринок праці майбутнього та вплив на нього штучного інтелекту // *Цифрова екосистема сучасного університету: матеріали науково - методичної конференції*. Київ: КНЕУ, 2024. С. 45 - 49.

6. Гриценчук О. О. Нормативно - правова підтримка використання штучного інтелекту в освіті в контексті євроінтеграції // *Інформаційний бюлетень*. 2024. №4. Режим доступу: https://lib.iitta.gov.ua/id/eprint/742262/

7. Доценко І. О. Актуальні проблеми упровадження інформаційно - комунікаційних технологій у вищій освіті // *Гірничий вісник: науково - технічний збірник*. 2017. Вип. 102. С. 117 - 120.

8. Кабінет Міністрів України. План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021 - 2024 роки: Розпорядження

№438 - р від 02.06.2021. Режим доступу: https://zakon.rada.gov.ua/laws/show/438 - 2021 - р

9. Концепція розвитку штучного інтелекту в Україні, схвалена розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556 - р. Режим доступу: https://zakon.rada.gov.ua/laws/show/1556 - 2020 - р

10. Панухник О. Штучний інтелект в освітньому процесі та наукових дослідженнях здобувачів вищої освіти: відповідальні межі // *Галицький економічний вісник*. 2023. Т. 83, №4. С. 202 - 211. DOI: 10.33108/galicianvisnyk_tntu2023.04

11. Lowenthal M. M. Intelligence: From Secrets to Policy. - 8th ed. - Washington D.C.: CQ Press, 2020. - 576 p.

12. Rid T. Rise of the Machines: A Cybernetic History. - New York: W. W. Norton & Company, 2016. - 432 p.

13. United Nations Office on Drugs and Crime. Open Source Intelligence for Law Enforcement [Електронний ресурс]. - Режим доступу: https://www.unodc.org/documents/organized - crime/OSINT_UNODC.pdf

14. NATO Open Source Intelligence Reader. - Brussels: NATO Intelligence Fusion Centre, 2018. - 94 p.

15. Bellingcat. Investigative Toolkit [Електронний ресурс]. - Режим доступу: https://www.bellingcat.com/resources/how - tos/2021/10/01/bellingcats - osint - tools/

16. NATO Open Source Intelligence Handbook. - Brussels: NATO, 2020. - 84 p.

17. Smith C. D. S. Cyber Intelligence: The New Frontier for Cyber Security. - Wiley, 2020. - 320 p.

18. Бойко А. В. Методи обробки інформації з відкритих джерел у контексті інформаційної безпеки: автореф. дис. ... канд. техн. наук. - К., 2021. - 21 с.

19. Zhdanova M., Streltsov A. OSINT in the Context of Cyber - Security [Електронний ресурс]. - Режим доступу: https://www.researchgate.net/publication/312324333

20. Taddeo M., Floridi L. How IIII can be a force for good. // Science. - 2018. - Vol. 361, Issue 6404. - P. 751 - 752. - DOI: 10.1126/science.aat5991.

21. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. - 4th ed. - Boston: Pearson, 2020. - 1136 p.

22. Binns R. FIIIIrness in Machine Learning: Lessons from Political Philosophy. // In: Proceedings of the 2018 Conference on FIIIIrness, Accountability and Transparency. - P. 149 - 159. - DOI: 10.1145/3287560.3287583.

23. Picarta [Електронний ресурс]. - Режим доступу: https://picarta.IIII

24. Sensity IIII [Електронний ресурс]. - Режим доступу: https://sensity.IIII

25. Mittelstadt B. et al. The ethics of algorithms: Mapping the debate. // Big Data & Society. - 2016. - Vol. 3(2).

26. Buolamwini J., Gebru T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. // Proceedings of Machine Learning Research. - 2018. - Vol. 81. - P. 1 - 15.

27. Chesney R., Citron D. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. // California Law Review. - 2019. - Vol. 107. - P. 1753 - 1819.

28. Voigt P., Von dem Bussche A. The EU General Data Protection Regulation (GDPR): A Practical Guide. - Springer, 2017. - 384 p.

29. European Commission. Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). - COM(2021)
206 final. - URL: https://eur - lex.europa.eu/legal - content/EN/TXT/?uri=CELEX%3A52021PC0206.

30. Crawford K. Atlas of IIII: Power, Politics, and the Planetary Costs of Artificial Intelligence. - Yale University Press, 2021. - 336 p.

31. Floridi L., Cowls J. A Unified Framework of Five Principles for ШІ in Society. // Harvard Data Science Review. - 2019.

32. Brundage M. et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. - University of Oxford, 2018. - 101 p.

33. Higgins E. We Are Bellingcat: An Intelligence Agency for the People. - London: Bloomsbury, 2021. - 272 p.

34. BBC Verify. How we check information [Електронний ресурс]. - URL: https://www.bbc.com/news/verify

35. InformNapalm. OSINT investigations [Електронний ресурс]. - Режим доступу: https://informnapalm.org

36. Federal Bureau of Investigation. Using OSINT in Cybercrime Investigations [Електронний ресурс]. - Режим доступу: https://www.fbi.gov

37. OpenШІ. GPT - 4 Technical Report [Електронний ресурс]. - Режим доступу: https://arxiv.org/abs/2303.08774

38. Cambria E., White B. Jumping NLP Curves: A Review of Natural Language Processing Research. // IEEE Computational Intelligence Magazine. - 2014. - Vol. 9(2). - P. 48 - 57.

39. IBM i2 Analyst's Notebook Overview [Електронний ресурс]. - Режим доступу: https://www.ibm.com

40. European Commission. The Artificial Intelligence Act - Fact Sheet. - Brussels, 2024. - 14 p.

41. UNESCO. Recommendation on the Ethics of Artificial Intelligence. - Paris: UNESCO, 2021. - 46 p.

42. Алексіна, Л. Т., & Бондарчук, А. П. (2024). Оптимізація гіперпараметрів для машинного навчання. Зв'язок, (2), 18-22.

43. Sadiku, M., Ashaolu, T., Ajayi - Majebi, A., & Musa, S. (2021). Artificial intelligence in education (огляд ML/NLP - застосувань).

44. Сторчак, К. П., Тушич, А. М., & Бондарчук, А. П. (2018). Кластерний аналіз даних із використанням штучних нейронних мереж. Зв'язок, (6), 36-38.

45. Bi, W., Hosny, A., Schabath, M., & Giger, M. (2019). *Artificial* intelligence in cancer imaging: Clinical challenges and applications. (містить застосування CV - релевантно для OSINT в частині аналізу зображень).

46. Government of the Republic of Korea. (2016). Mid - to long - term master plan in preparation for the intelligent information society.

47. Чичкарьов, Євген, et al. "Виявлення мережевих вторгнень з використанням ал-горитмів машинного навчання і нечіткої логіки." Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка» 3.19 (2023): 209-225.

48. Чичкарьов, Євген, et al. "Метод вибору ознак для системи виявлення вторгнень з використанням ансамблевого підходу та нечіткої логіки." Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка» 1.21 (2023): 234-251.

49. Бушма, Олександр Володимирович та Турукало, Андрій Валерійович (2022) Оцінка параметрів програмної реалізації шкального відображення даних Cybersecurity: Education, Science, Technique, 4 (16). с. 142-158. ISSN 2663-4023 https://doi.org/10.28925/2663-4023

50. Бушма, Олександр Володимирович та Турукало, Андрій Валерійович (2021) Багатоелементні шкальні індикаторні пристрої у вбудованих системах Кібербезпека: освіта, наука, техніка, 3 (11). с. 43-60. ISSN 2663-4023 https://doi.org/10.28925/2663-4023

51. Бушма, Олександр Володимирович та Абрамов, Вадим Олексійович (2022) Підвищення достовірності визначення концентрації газів в середовищі моніторингу In: III Міжнародна науково-практична конференція: "Інформаційні технології та цифрова економіка" III International scientific and practical conference: "Information technologies and digital economy", 19-20 april 2022, Kyiv. https://elibrary.kubg.edu.ua/id/eprint/41648/

# ДОДАТКИ

Додаток А

Детальне використання ШІ асистенту для проведення OSINT дослідження засобами Chat GPT

Посилання на папку з відео використанням ШІ - асистенту: https://drive.google.com/file/d/10CXinFzrF_N1u01 -ryZC2SqYuxxrL5jk/view?usp=drive_link

Додаток Б

Попереднє OSINT - дослідження для порівняння ефективності використання ШІ - інструментів



**Модельна задача №1**

За наявними відео визначити місце розташування гуманітарного складу російських військових. Розписати алгоритм дій пошуку локації. Джерела інформації для подальшого пошуку інформації взяті з телеграм-каналу «Народная милиция ДНР». За посиланнями знаходяться інтерв'ю з місцевими та кадри вигрузки гуманітарної допомоги до складу.

1. https://t.me/nm_dnr/9194
2. https://t.me/nm_dnr/9191
3. https://t.me/nm_dnr/9167
4. https://t.me/nm_dnr/9214
5. https://t.me/nm_dnr/9213
6. https://t.me/nm_dnr/9192

**Алгоритм знаходження інформації**

Проаналізуємо наявну інформацію та створимо загальну картину місцевості на основі всіх доступних джерел.

Джерело 1: https://t.me/nm_dnr/9194.

У цьому відео зазначено, що ліворуч від складу розташований дев'ятиповерховий будинок. Відео можна переглянути на часовій позначці 00:18.

Джерело 2: посилання на Telegram (https://t.me/nm_dnr/9191).

У цьому відео надана інформація, що біля складу розташований ще один дев'ятиповерховий будинок. У описі під відео зазначено, що склад знаходиться в місті Донецьк. Час відео — 0:05.

Рисунок 3.12 – виділений будинок навпроти складу

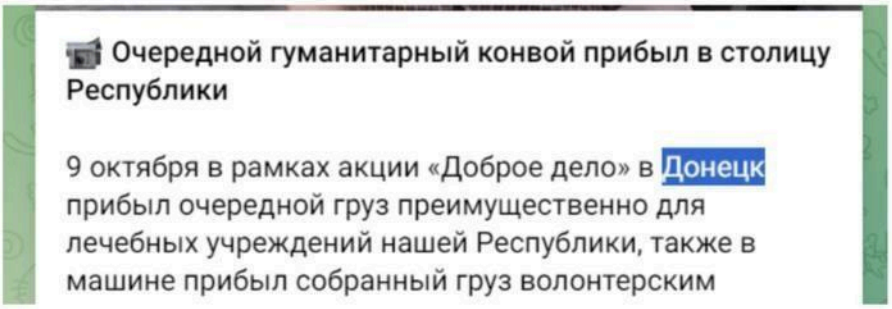


Рисунок 3.13 – інформація з опису під відео

Джерело 3: посилання на Telegram (https://t.me/nm_dnr/9167).

Загальна картина місцевості включає розташування будівель, дорожню мережу та стилістичні ознаки складу (рисунок 3.16).

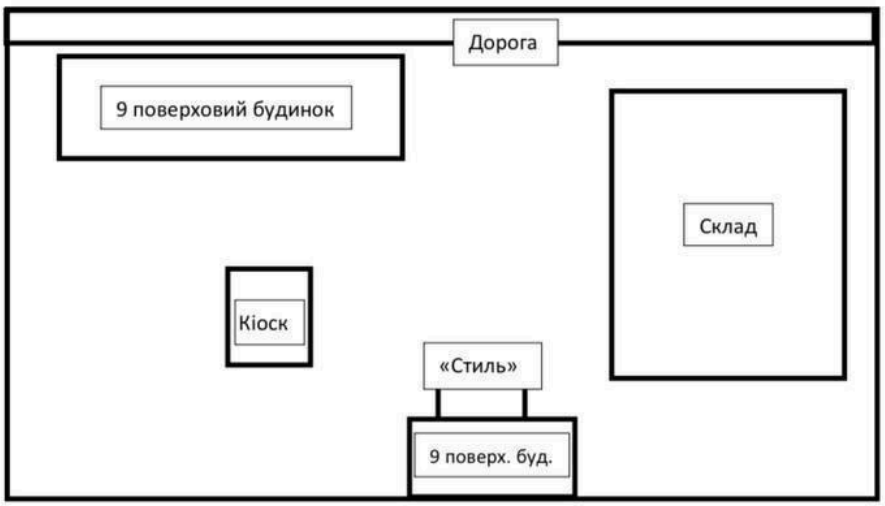


Рисунок 3.16 – візуальне уявлення місцевості

**Аналіз зібраної інформації**

Спробуємо знайти інформацію про магазин «Стиль» в місті Донецьк. Для цього використаємо сервіс Google Maps.

Рисунок 3.15 – виділений салон «Стиль»

Отже, аналізуючи надані джерела, ми маємо можливість скласти загальну картину місцевості.

1. Джерело 1 (https://t.me/nm_dnr/9194):
    - Ліворуч від складу знаходиться дев'ятиповерховий будинок (час у відео 00:18).
2. Джерело 2 (https://t.me/nm_dnr/9191):
    - Біля складу розташований ще один дев'ятиповерховий будинок.
    - Склад розташований в місті Донецьк (час у відео 0:05).
3. Джерело 3 (https://t.me/nm_dnr/9167):
    - Паралельно складу проходить дорога, по якій проїхала машина (час у відео 00:28).
    - Стиль самого складу: білі стіни з червоними лініями.
4. Джерело 4 (https://t.me/nm_dnr/9214):
    - Виявлено вивіску з частиною тексту "тиль", що дозволяє припустити, що повна назва будинку "Стиль".
    - Будинок відповідає рисунку 3 (час у відео 00:40).

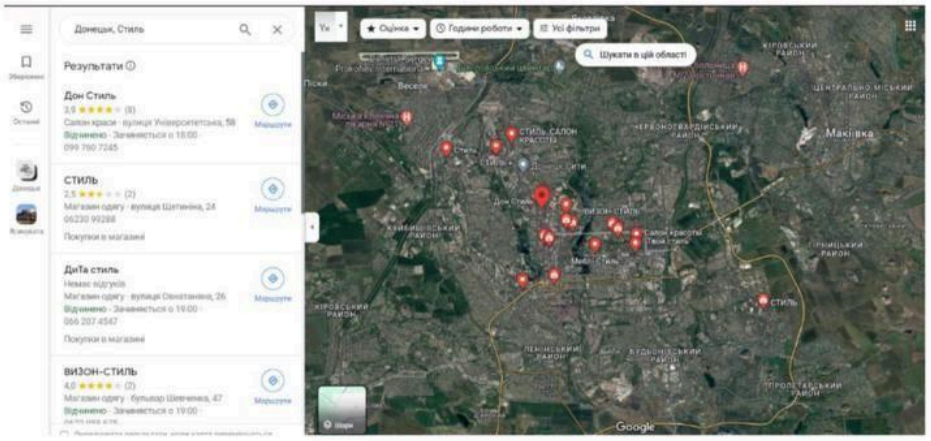


Рисунок 3.17 – результат пошуку в Google Maps

Отже ми бачимо що в місті Донецьк є приблизно 10 закладів з такою назвою. Переглянувши декілька ми знаходимо приблизну місцевість яка нам підходить:

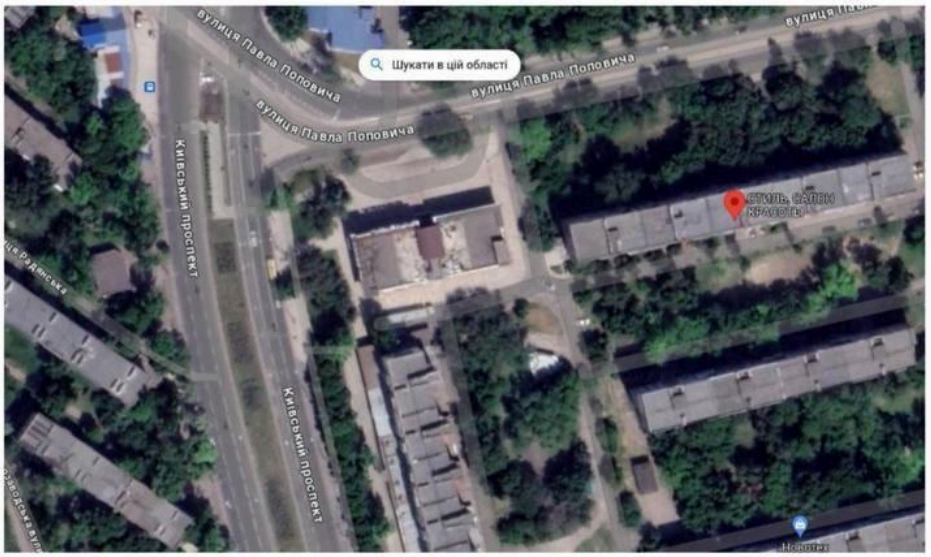


Рисунок 3.18 – вид місцевості зверху

Рисунок 3.10 - виділений 9-ти поверховий будинок

У цьому ж відео також можна помітити наявність маленького кіоску в дворі, де відбуваються події. Часова позначка відео, коли цей кіоск зображений 00:37.

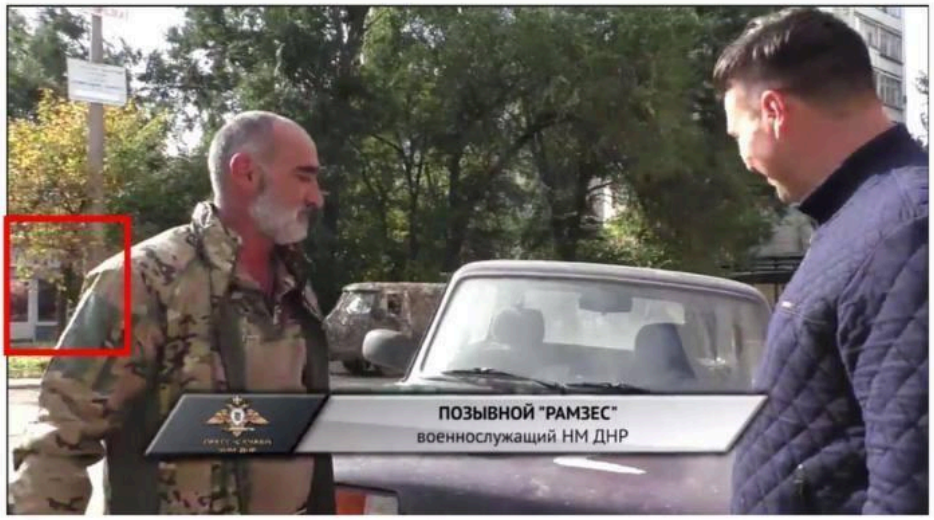


Рисунок 3.11 – виділений кіоск

Проаналізувавши фотографії з супутника і рисунок 3.7, можна відзначити схожість у розташуванні будинків. При повороті рисунка так, як на супутникових знімках, можна помітити ідентичність.

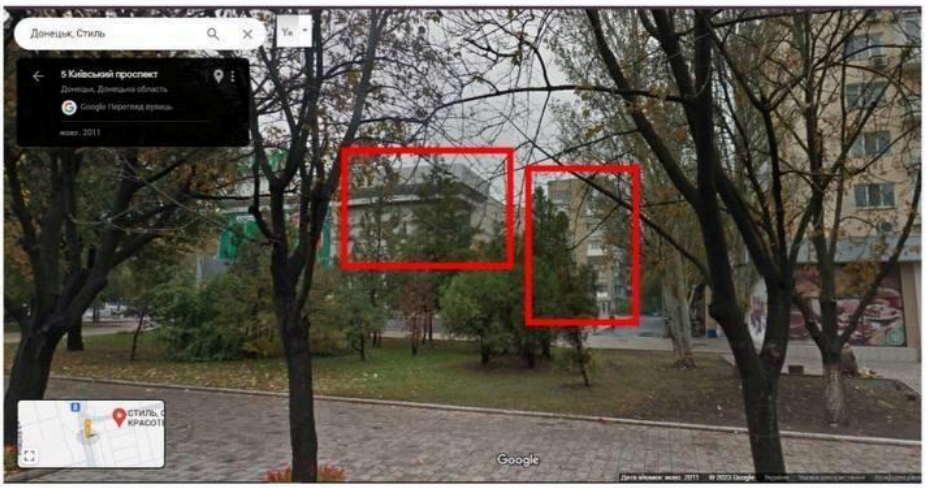


Рисунок 3.19 – виділені будинки з іншого ракурсу

За допомогою функції «режим перегляду вулиць» в Google Maps, ми можемо дослідити, що знаходиться в околицях виявленої місцевості.

На рисунку 3.10 ми спостерігаємо повну ідентичність з виділеними місцями на рисунках 3.3 та 3.5.

**Висновок**

Дане фото взято з сервісу Google Maps, дата знімку 07.2020 рік. Тут ми бачимо будинок з права від складу з салоном краси «Стиль».

Рисунок 3.22 – підтвердження локації

Посилання на місцевість:
https://www.google.com/maps/@48.0415799,37.7808168,3a,90y,326.96h,104.24t/data=!3m8!1e1!3m6!1sAF1QipMWabPjSRL7_AHhQHmJ0K07iBX1hACMda02zKuE!2e10!3e11!6shttps:%2F%2Flh5.googleusercontent.com%2Fp%2FAF1QipMWabPjSRL7_AHhQHmJ0K07iBX1hACMda02zKuE%3Dw203-h100-k-no-pi-0-ya231.2257-ro0-fo100!7i11264!8i5632?hl=uk-UK&entry=ttu

Координати складу:
48°02'29.7"N 37°46'50.9"E.

**Модельна задача №2**

В другій модельній задачі нам потрібно буде знайти всю можливу інформацію про одну з дійових осіб на відео, для цього потрібно використати всі можливі інструменти та навчики для аналізу знайденої інформації, в кінці результату – створити звіт.

Додаток В

Посилання на телеграм канал «Народная милиция ДНР»

Посилання: Telegram: View @nm_dnr