

Олександр КОРИСТІН

Сергій ДЕМЕДЮК



OSINT

OPEN SOURCE INTELLIGENCE

КНИГА 2

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

Олександр КОРИСТІН

Сергій ДЕМЕДЮК

OSINT OPEN SOURCE INTELLIGENCE

Інструменти та методи

*Видано за підтримки
CRDF Global в Україні*



УДК 004.056.5:351.861:351.746.1(075)

О 73

DOI: 10.32782/osint-instruments-2025

Рекомендовано до друку:

вченою радою Одеського державного університету внутрішніх справ
(протокол № 11 від 26 серпня 2025 року)

Рецензенти:

Корченко О. Г. – член-кореспондент НАН України, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, заслужений діяч науки і техніки України;

Корнієнко М.В. – доктор юридичних наук, професор;

Мовчан А.В. – доктор юридичних наук, професор.

OSINT Open Source Intelligence. Інструменти та методи: навчальний посібник / Користін О., Демедюк С., Ісмаїлов К., Ланде Д. та ін., за заг. ред. Користіна О.Є., Демедюка С.В. – Київ: 7БЦ, 2025. 460 с.

ISBN 978-617-8794-17-0

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

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

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

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

УДК 004.056.5:351.861:351.746.1(075)

ISBN 978-617-8794-17-0

ПРОМПТ ІНЖИНІРИНГ НА ОСНОВІ БЕЗКОДОВОГО ПРОГРАМУВАННЯ

Дмитро ЛАНДЕ
Leonard STRASHNOY

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

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

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

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

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

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

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

автоматизованих аналітичних процесах.

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

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

КОНЦЕПЦІЯ БЕЗКОДОВОГО ПРОГРАМУВАННЯ

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

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

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

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

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

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

РОЗДІЛ 15

ВИКОРИСТАННЯ LLM&PYTHON В OSINT РОЗСЛІДУВАННЯХ

Олексій БАРАНОВСЬКИЙ

YOLOV8 ДЛЯ РОЗПІЗНАВАННЯ ОБ'ЄКТІВ

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

Що таке YOLOv8?

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

Ключові можливості

Модель має широкий спектр застосувань. Основні можливості включають:

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

Практичний приклад: Аналіз фото із соціальних мереж

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

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

Кроки виконання (локальний запуск через Python):

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