Список використаних джерел:

1. Лотюк О.С. Конституційні засади обмеження прав та свобод людини і громадянина у повоєнний період. *Актуальні проблеми вітчизняної юриспруденції*. 2023. № 2. С. 9-15.
2. Коба М.М. Обмеження прав і свобод людини в умовах війни: загальнотеоретичний аналіз. *Juris Europensis Scientia*. 2024. Вип. 4. С.8-14.
3. Кубаєнко А., Крижановська О., Курганський О. Сучасні практики поліцейської діяльності: навчально-методичний посібник. Нац. ун-т «Одеська юридична академія». Одеса: Юридична література, 2024. 144 с.
4. Главацька А. О., Ангельська О. В., Опірський І. Р. Дослідження технології використання OSINT // Матеріали науково-практичної конференції. 2024.

ДЕЯКІ ОСОБЛИВОСТІ ВИКОРИСТАННЯ OSINT-ІНСТРУМЕНТІВ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ФЕЙКОВИХ НОВИН ТА ДЕЗІНФОРМАЦІЇ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Савенко Дмитро Олександрович
старший інспектор 5-го відділу 3-го управління
Департаменту кіберполіції Національної поліції України
Ісмайлов Карен Юрійович
кандидат юридичних наук, доцент,
начальник 5-го відділу 3-го управління
Департаменту кіберполіції Національної поліції України

Актуальність дослідження визначається тим, що на сьогоднішній день першочерговим обов'язком держави, особливо в умовах воєнного стану, залишається забезпечення безпеки її громадян. Спектр загроз національній безпеці стає все більш складним та різноманітним. Тероризм, кібератаки, нетрадиційні атаки із застосуванням хімічної, ядерної або біологічної зброї, а також масштабні аварії або природні катаклізми - будь-що може поставити під загрозу безпеку громадян, завдавши серйозної шкоди інтересам та економічному добробуту країни [1, с. 21]. В умовах стрімкого розвитку інформаційних технологій виникла принципово нова категорія загроз:

дезінформаційні кампанії, розповсюдження фейкових новин та інформаційно-психологічні операції (ІПСО).

Метою дослідження є аналіз технічних можливостей сучасних OSINT-інструментів на основі штучного інтелекту в контексті виявлення фейкових новин та протидії дезінформаційним кампаніям, а також визначення особливостей їх практичного застосування в умовах гібридної війни в контексті російсько-українського збройного конфлікту.

Особливої гостроти ця проблематика набуває після початку повномасштабного вторгнення росії у 2022 році, де країна-агресор системно використовує інформаційно-психологічні операції як повноцінний інструмент ведення гібридної війни, що застосовується паралельно з традиційними бойовими діями. Основною метою таких операцій є дестабілізація внутрішньополітичної ситуації в Україні, психологічний тиск на населення та провокування соціальних конфліктів.

За таких умов дослідження технічних засобів виявлення та нейтралізації дезінформаційних загроз, зокрема OSINT-інструментів на основі штучного інтелекту, набуває не лише наукового, а й практичного значення для забезпечення інформаційної безпеки держави.

Основні загрози, які несуть інформаційно-психологічні операції в умовах воєнного конфлікту: розпалення конфлікту та поглиблення напруження, маніпуляція суспільною думкою, розповсюдження дезінформації, підрив моралі та деморалізація військових та населення, психологічний тиск та зміна стратегій ведення війни, посилення стереотипів та ворожнечі, порушення міжнародного співтовариства [2, с. 9].

З початку XXI століття в умовах технологічного прогресу Інтернет давно вже міцно увійшов у життя людей, а для деяких осіб – це єдиний спосіб самовираження та пошуку друзів або заработка. Завдяки створенню Інтернету, кожна людина може приєднатися до величезних і практично невичерпних джерел інформації [3, с. 132]. Саме тому розвідка з відкритих джерел грає дуже важливу роль в сучасному світі.

Роль OSINT в кібербезпеці є комплексною. Для приватної особи OSINT – це спосіб побачити себе очима зовнішнього світу, а також для захисту особистої ідентичності в Інтернеті [4, с. 49]. Для держави - це механізм, який одночасно виступає як інструмент для збору розвідувальної інформації, так і для протидії вище

зазначеним діям з боку іншого суб'єкту (країна-агресор, тощо), особливо в контексті поширення дезінформації, фейків та ІПСО.

За умов стрімкого розвитку інформаційних технологій розвідка з відкритих джерел залишається одним із найбільш перспективних та багатосторонніх інструментів у сфері кібербезпеки. Інформація отримана за допомогою розвідки з відкритих джерелах може одночасно використовуватись як інструмент протидії загрозам національній безпеці України, так і як інструмент для їх розповсюдження, наприклад: розповсюдження інформації про об'єкти критичної інфраструктури, військові об'єкти та інші чутливі підприємства [5, с. 169]. В контексті поширення фейкових новин та дезінформації OSINT-інструменти також можуть використовуватися як з метою розповсюдження такої інформації, так і для протидії проти неї.

Як було зазначено раніше, особливу загрозу національній безпеці становить розповсюдження дезінформації (системна, цілеспрямована діяльність із поширення хибних або маніпулятивних відомостей з метою досягнення конкретного політичного, військового чи соціального ефекту) та фейків (конкретна одиниця неправдивого контенту: сфабрикована новина, підроблене зображення, вирване з контексту відео, тощо), що в свою чергу може сприяти зміні соціальних настроїв та спонуканню населення країни до певних діянь. Тобто, збір відкритої інформації, включно з аналізом соціальних мереж, супутникових знімків, повідомлень у ЗМІ та даних із різних онлайн-ресурсів, є важливим елементом боротьби проти дезінформації [6, с. 283].

У світі, де відкриті джерела інформації є основними джерелами комунікації, використання OSINT технологій для збору даних створює не лише можливості, але й серйозні загрози [7, с. 242]. Саме тому слід приділити особливу увагу взаємодії OSINT з технологіями штучного інтелекту (ШІ) у боротьбі з дезінформацією. Сучасні рішення на основі ШІ, такі як автоматизовані системи перевірки фактів, виявлення контенту типу «deepfake» на основі нейронних мереж та алгоритми кластеризації скоординованих інформаційних кампаній, значно посилюють аналітичний потенціал OSINT [8, с. 111]. Інтеграція розвідки з відкритих джерел та машинного навчання створює нову парадигму боротьби з гібридними інформаційними загрозами, що у свою чергу вимагає відповідної правової кодифікації у національному законодавстві та міжнародних угодах, які стосуються кіберпростору.

Станом на сьогодні існує достатньо велика кількість ШІ-інструментів, які доцільно використовувати під час перевірки новин та протидії дезінформації як працівникам державних структур, так і приватним підприємствам:

Назва	**Технічні можливості OSINT-інструменту**
Hive AI	Детектор згенерованого ШІ-контенту (зображення, текст, відео). Використовує ансамблі CNN, класифікує ймовірність AI-генерації у відсотках. API-доступ, пакетна обробка. Окремі моделі для DALL-E, Midjourney, Stable Diffusion.
Decopy AI	Реверсний пошук зображень + детектор AI-генерації. Пошук за візуальним fingerprint-ом через перцептивний хешинг. Виявляє часткові копії та маніпуляції (обрізка, накладення фільтрів).
TinEye	Реверсний пошук зображень на базі власного індексу (60+ млрд зображень). Використовує image fingerprinting, а не метадані. Відстежує хронологію появи зображення в мережі — дозволяє знайти оригінальне джерело.
InVID-WeVerify	Браузерний плагін для верифікації відео та зображень. Розбиває відео на keyframe-и, запускає реверсний пошук по кожному. Аналізує метадані, геолокацію, контекст публікації. Інтегровано з YouTube Data API.
Deepware scanner	Спеціалізований детектор deepfake-відео. Аналізує артефакти на рівні облич (blending boundaries, temporal inconsistencies). На вході — URL або файл, на виході — score ймовірності маніпуляції.
AI voice detector	Бінарний (score-based) класифікатор синтезованої мови. Аналізує спектральні характеристики, просодику, артефакти TTS-моделей. Деякі версії розрізняють конкретні TTS-движки.
Let`s Data	No-code платформа для збору та аналізу публічних даних (соцмережі, веб). Парсинг без API, побудова датасетів, базова аналітика + інтеграція з BI-інструментами. Орієнтована на OSINT-журналістику.
Pangram	Детектор AI-тексту з фокусом на провенанс контенту. Використовує watermarking-сигнали та статистичний аналіз розподілу токенів. Позиціонується для медіа та академічного середовища.

Таб. Порівняння технічних можливостей OSINT інструментів на основі ШІ

одночас, формування належного інформаційно-безпекового середовища для здійснення OSINT-діяльності супроводжується низкою суттєвих організаційно-технічних та правових проблем. Водночас відсутність уніфікованих стандартів і методичних рекомендацій щодо побудови подібної інфраструктури призводить до фрагментарності підходів та підвищує ризики інформаційної безпеки [9, с. 156].

Таким чином, проведений аналіз дозволяє сформулювати наступні висновки: по-перше, розвідка з відкритих джерел в поєднанні з інструментами штучного інтелекту сформувала якісно новий рівень верифікації інформації: автоматизовані детектори (Hive AI, Deepware Scanner, AI Voice Detector) дозволяють виявляти згенерований або маніпульований контент у режимі реального часу, що раніше вимагало значних людських ресурсів та часових витрат.

По-друге, повномасштабне вторгнення росії в лютому 2022 року стало каталізатором масштабного впровадження OSINT-інструментів: їх використання вийшло за межі академічного та журналістського середовища та поширилося на рівень державних структур та збройних сил. Це підтверджує, що OSINT-інструментарій перестав бути допоміжним і набув статусу самостійного елемента системи національної безпеки.

По-третє, жоден з розглянутих інструментів не є універсальним: кожен із них орієнтований на конкретну модальність контенту (текст, зображення, відео, аудіо), що обумовлює необхідність їх комплексного використання в рамках єдиної верифікаційної методології.

По-четверте, чинне законодавство України не містить спеціальних норм, що регулюють застосування OSINT-інструментів на основі ШІ у сфері протидії дезінформації, що створює правову невизначеність щодо допустимості зібраних доказів та відповідальності суб'єктів розвідувальної діяльності. Усунення цієї прогалини є необхідною умовою для інституціоналізації OSINT-практик на державному рівні.

Список використаних джерел:

1. Користін О.Є., Демедюк С.В. OSINT Open Source Intelligence. Теорія та методологія : монографія. Київ : 7БЦ, 2025. 304 с.

2. Ісмайлов К.Ю. Роль інформаційно-психологічних операцій в сьогоденні: проблематика, виклики та заходи захисту.

Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика: матеріали Міжнародної науково-практичної конференції (м. Одеса, 24 листопада 2023 р.). Одеса, 2023. С. 8-10.

3. Ісмайлов К.Ю. Інтернет як сучасний фактор розповсюдження дискримінаційних виявів. *Порівняльно-аналітичне право.* 2017. № 3. С. 131-133.

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

5. Івкова В.С., Опірський І.Р. OSINT-технології як загроза кібербезпеці держави. *КІБЕРБЕЗПЕКА: освіта, наука, техніка*. 2025. Т. 3, № 27. С. 165-179.

6. Величко Т.О. Протидія російській інформаційній агресії за допомогою OSINT. *Оперативно-бойова діяльність сил сектору безпеки і оборони в умовах воєнного стану* : Матеріали Всеукр. науково-практ. конф. представників сектору безпеки і оборони України, наук. та науково-пед. працівників, здобувачів освіти та інших зацікавл. осіб, м. Київ, 24 жовтня 2024 р. Київ, 2024. С. 283-284.

7. Савенко Д.О., Ісмайлов К.Ю. OSINT та соціальні мережі: загрози та можливості для молодіжних комунікацій. *«Sociological and psychological models of youth communication»*: VII Міжнародна науково-практична конференція, Copenhagen, 18-21 February 2025. С. 242-246.

8. Ісмайлов К.Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації. *Південноукраїнський правничий часопис*. 2016. № 2. С. 110-113.

9. Ісмайлов К.Ю. Деякі особливості нормативного регулювання діяльності правоохоронців у мережі інтернет в Україні. *Актуальні питання діяльності Національної поліції як суб'єкту протидії організованій злочинності* : матеріали Всеукраїнської науково-практичної конференції (м. Кропивницький, 02 квітня 2026 року). Кропивницький, 2026. С. 154-157.