

соціальної держави, має в Україні значний консолідуючий потенціал і надає більше можливостей для конструювання макрополітичної ідентичності, ніж модель, заснована на ідеях романтичного націоналізму [3].

Оскільки впровадження політики ідентичності вимагає врахування широкого спектра політичних, соціокультурних і правових чинників, досвід інших країн не можна сприймати як набір готових рішень. Унікальність кожного суспільства зумовлює необхідність суттєвої адаптації запозичених підходів до власних реалій. Водночас порівняльний аналіз та зміна перспективи можуть забезпечити відчутний позитивний ефект, що, у свою чергу, дозволяє розробити конкретні рекомендації для вдосконалення процесу формування макрополітичної ідентичності.

1. Проблеми формування спільної ідентичності громадян України в оцінках експертів. Національна безпека і оборона. 2007. № 9 (93). С. 45–52.
2. Процес формування спільної загально-національної ідентичності громадян : чинники впливу, основні засади і напрями. Національна безпека і оборона. 2017. № 1–2. С. 77–88.
3. Мендрін О. В. Формування макрополітичної ідентичності як фактор сталості демократичного розвитку в Україні. Вісник Маріупольського державного університету. Серія : Історія. Політологія. 2020. № 28–29. С. 242–251. DOI: 10.34079/2226-2830-2020-10-28-29-242-251.



Едуард РИЖКОВ
професор кафедри
інформаційних технологій
Дніпровського державного
університету внутрішніх справ
(м. Дніпро, Україна),
кандидат юридичних наук, професор
<https://orcid.org/0000-0002-6661-4617>

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ OSINT

Технологія OSINT (Open Source Intelligence) набуває свого поширення і вдосконалення темпами, притаманними розвитку інформаційних технологій у сучасному світі. З метою отримання інформації з відкритих джерел її дедалі активніше використовують від сфери військової розвідки, оперативного-розшукової діяльності правоохоронних органів до бізнесу і розваг. В Україні цей інструмент успішно використовується також підрозділами кримінального аналізу Національної поліції, де він демонструє високу ефективність у зборі, аналізі та систематизації даних. Використання штучного інтелекту (далі – AI) при реалізації OSINT відкриває нові перспективи для підвищення ефективності кримінального аналізу, оптимізації навчальних процесів та забезпечення оперативного реагування на прояви злочинності.

В Україні розпочато процес правової регламентації використання штучного інтелекту [1]. Але ми погоджуємося із твердженнями фахівців про недосконалість правового регулювання штучного інтелекту як в Україні, так і за кордоном [2, с. 149].

Отримання інформації з відкритих джерел компенсує і доповнює можливості розвідувальної та оперативного-розшукової діяльності, а інколи здатне їх повністю або частково замінити. Пошук, фіксація, перевірка, аналіз і синтез інформації можуть проводитись у «ручному режимі», а можуть бути певною мірою автоматизовані. Штучний інтелект дозволяє значно прискорити процес обробки даних, автоматизуючи рутинні процеси та забезпечуючи точність і релевантність отриманої інформації. Завдяки цьому правоохоронні органи можуть швидше ідентифікувати підозрюваних, встановлювати зв'язки між особами, аналізувати потенційні загрози, розкривати злочини та досягати успіхів у розшуковій та пошуковій роботі [3, с. 38].

OSINT дозволяє отримувати необхідну інформацію про осіб і факти, які становлять оперативний інтерес, без суттєвих обмежень, які характерні для опрацювання закритих джерел або при використанні можливостей оперативного-розшукової діяльності та розвідки. За допомогою AI стає можливим автоматизований моніторинг соціальних мереж, новинних

ресурсів, форумів та інших онлайн-платформ. Це дає змогу оперативно отримувати актуальні дані, знижуючи витрати часу та інших ресурсів.

OSINT доповнює оперативно-розшукову діяльність та класичну розвідувальну діяльність, які мають чітке нормативно-правове регулювання в Україні. Законодавство, зокрема Конституція України та Кримінальний процесуальний кодекс України (далі – КПК), визначає необхідність дотримання прав і свобод людини під час збору інформації. Наприклад, статті 31, 32 Конституції України гарантують недоторканність приватного життя, а статті 159–164 КПК регулюють порядок отримання доступу до інформації. AI може допомогти зберегти баланс між оперативністю збору інформації та обмежувальним та стримуючим дотриманням правових норм, пропонуючи інструменти автоматичного аналізу даних без порушення законодавства.

У контексті війни між Україною та РФ використання штучного інтелекту для OSINT дозволяє AI швидко обробляти великі обсяги інформації, знаходити кореляції між даними та фільтрувати шум. Моделі, такі як GPT, Gemini, DeepSeek та інші можуть розшифровувати складні повідомлення та аналізувати текст. AI, крім іншого, допомагає визначати фейкові акаунти та дезінформацію. Однак сам AI також може стати (і вже ефективно використовується) інструментом для поширення пропаганди та фейків в інтересах України. AI дозволяє виявляти мережі ботів і відстежувати наративи, які розповсюджують ворожу пропаганду. Його успішно можна використовувати для розробки нових алгоритмів виявлення інформаційних операцій. Військові та правоохоронці можуть використовувати AI для аналізу активності у соцмережах, визначення локацій та ідентифікації підозрілих груп. Комп'ютерний зір дозволяє аналізувати супутникові знімки, відео та фотографії.

Необхідну допомогу Україні з урахуванням військових та правоохоронних потреб надають міжнародні фахівці у сфері використання AI та OSINT. Так, засновники Clearview AI констатували, що їх стартап на початок повномасштабного вторгнення мав у своєму розпорядженні понад два мільярди зображень з російської соціальної мережі «ВКонтакте», а загальна база даних налічувала понад 10 мільярдів фотографій, які пропонувалися для успішного використання при розкритті воєнних злочинів [4].

У постійному пошуку найновіших та нестандартних рішень перебувають вітчизняні профільні міністерства. Зокрема, керівник одного з них зазначає, що штучний інтелект – саме така технологія, яка зараз дає Україні перевагу на полі бою: завдяки штучному інтелекту (крім іншого – Р.Е.) на мапі з'являються об'єкти та цілі [5].

Також прикладом є автоматичне розпізнавання військової техніки чи руху колон. Застосування AI для аналізу геопросторових даних дозволяє отримувати інформацію про пересування військ у режимі реального часу.

З 2014 року OSINT став надзвичайно важливим для українських військових, волонтерів та правоохоронців. Такі проєкти, як InformNapalm та Bellingcat, Molnar та інші за 10 років війни довели ефективність OSINT як окремо, так і в гармонійному поєднанні з AI, стрімкий розвиток якого спостерігаємо з 2022 року.

Переконані в тому, що з урахуванням воєнного стану в Україні та інших країнах світу військові та правоохоронці все частіше будуть використовувати AI для OSINT як найближчим часом, так і надалі. Розвиток штучного інтелекту, конкуренція між розробниками його різноманітних платформ створює сприятливе середовище для вдосконалення цієї технології. Можна очікувати створення новітніх спеціалізованих AI-платформ для автоматизованої обробки інформації на більш сучасному рівні.

У питанні вдосконалення підготовки кадрів для правоохоронних органів штучний інтелект здатен компенсувати нестачу навчального часу під час підготовки, наприклад, майбутніх працівників оперативних підрозділів кримінальної поліції або працівників підрозділів кримінального аналізу України.

Під час вивчення навчальної дисципліни з OSINT штучний інтелект за оперативним запитом може пропонувати якісні алгоритми дій, надавати рекомендації щодо використання конкретних програмних продуктів і платформ, а також допомагати з їх налаштуванням на комп'ютерах та інших пристроях. Застосування таких інструментів, як Maltego, IBM Watson Discovery, Planet AI + Google Earth Engine, DeepVision AI, Hootsuite Insights (на основі AI), Clearview AI та інших, а також спеціалізованих вебсервісів, наприклад для аналізу соціальних мереж, дозволяє швидко освоїти методики роботи із пошуком інформації, з самою інформацією та ефективно використовувати їх у практичній діяльності.

Актуальним з практичних міркувань є питання, чи зможе в перспективі штучний інтелект повністю замінити фахівця під час проведення OSINT?

Ми дотримуємося такої позиції, що з часом AI буде здатен реалізувати автономну функцію після отримання завдання лише на початкових та проміжних стадіях OSINT. Він також є незамінним для початківців у методичному плані, під час розробки тактики та стратегії відпрацювання конкретного завдання. Початкова аналітика також може проводитись AI самостійно. Завершальна стадія OSINT однозначно потребує і надалі буде потребувати участі фахівця.

Отже, перспектива використання штучного інтелекту під час реалізації технології OSINT в Україні з урахуванням воєнних та правоохоронних потреб є реальною та пріоритетною.

Ця технологія у гаймонічному поєднанні з AI не лише дозволяє отримувати цінну інформацію з відкритих джерел, доповнювати оперативно-розшукову та розвідувальну діяльність, а також підвищує ефективність самого кримінального аналізу.

В умовах постійного розвитку інформаційних технологій штучний інтелект стає незамінним інструментом для забезпечення національної безпеки та протидії злочинності. Тому потребує додаткового вивчення в межах окремої навчальної дисципліни або спеціалізованих тем під час підготовки профільних фахівців через вдосконалення навчальних планів.

1. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text>.

2. Зачек О. І., Дмитрик Ю. І., Сенік В. В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ. Серія : Юридична*. 2023. Вип. 3. С. 148–156.

3. Рижков Е. В., Писаренко Н. Ю. Штучний інтелект як аналітичний інструмент для розкриття кримінальних правопорушень. *Актуальні питання забезпечення діяльності органів і підрозділів системи МВС технічними засобами в умовах воєнного стану : матеріали II всеукр. науково-практ. конф. (м. Київ, 25 квітня 2024 р).* Київ : ДНДІ МВС, 2024. С. 38–39.

4. Міноборони України почало використовувати систему розпізнавання облич Clearview AI. URL: <https://dou.ua/forums/topic/37142/>.

5. Як Україна використовує штучний інтелект для перемоги. У Мінцифри розповіли деталі. URL: <https://dou.ua/lenta/news/clearview-ai-in-ukraine/>.



Анна ІЛЬЄНКО
завідувач кафедри
кібербезпеки,
кандидат технічних
наук, доцент

<https://orcid.org/0000-0001-8565-1117>



Валентина ТЕЛЮЩЕНКО
асистент,
аспірант кафедри
кібербезпеки

<https://orcid.org/0000-0001-6026-5105>

(Державний університет «Київський авіаційний інститут»,
м. Київ, Україна)

МЕТОДИ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРЗАГРОЗ У КРИТИЧНІЙ ІНФРАСТРУКТУРІ

В Україні забезпечення національної безпеки є одним із пріоритетних завдань державної політики, включно із захистом об'єктів критичної інфраструктури (ОКІ). У зв'язку з постійними викликами, зокрема військовою агресією, кібератаками та економічними загрозами, наша країна активно розвиває механізми захисту стратегічно важливих об'єктів. Тому оцінювання ризиків кіберзагроз є одним із основних аспектів забезпечення надійної роботи ОКІ, що дозволяє виявити вразливості, прогнозувати потенційні атаки та мінімізувати їх наслідки.

Мета дослідження: аналіз та порівняння сучасних методів оцінювання ризиків кіберзагроз у критичній інфраструктурі, виявлення їхніх переваг та недоліків, а також