УДК / UDC: 327.56
DOI: https://doi.org/10.37750/2616-6798.2026.1(56).357368

Олександр Володимирович Сушко
Міжрегіональна академія управління персоналом, Науково-навчальний інститут права та безпеки імені князя Володимира Великого
Київ, Україна
ORCID: https://orcid.org/0009-0008-2602-6328
Іван Васильович Сервецький
Міжрегіональна академія управління персоналом, Науково-навчальний інститут права та безпеки імені князя Володимира Великого
Київ, Україна
ORCID: https://orcid.org/0000-0002-5713-8911

ОЗНАКИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У РОЗВІДУВАЛЬНІЙ ДІЯЛЬНОСТІ

Анотація. *У статті досліджено ознаки, що свідчать про використання технологій штучного інтелекту (ШІ) у діяльності розвідувальних спецслужб. Проаналізовано типові маркери — як технічні, так і поведінкові, що дозволяють ідентифікувати застосування масштабованої аналітики, автоматизованого збору та класифікації даних, синтетичних медіа й інтелектуальної підтримки прийняття рішень. Методологія дослідження поєднує огляд відкритих джерел (OSINT), порівняльний аналіз задокументованих інцидентів та узагальнення зовнішніх індикаторів (анонімізовані кейси, патерни трафіку й публікацій). Виокремлено ключові категорії ознак: масштабність і швидкість аналітичних висновків, регулярність та одноманітність повідомлень, поява синтетичного або трансформованого контенту (deepfake, генеративні тексти), адаптивні поведінкові моделі контактів і кампаній, а також міжплатформна координація дій. Розглянуто ризики для національної безпеки, етичні та правові аспекти використання ШІ у розвідці, а також запропоновано загальні напрями моніторингу й формування політик протидії.*

Ключові слова: *розвідка, штучний інтелект, OSINT, синтетичні медіа, індикатори використання ШІ, національна безпека.*

Oleksandr V. Sushko
Interregional Academy of Personnel Management, Educational and Scientific Institute of Law and Security named after Prince Volodymyr the Great
Kyiv, Ukraine
ORCID: https://orcid.org/0009-0008-2602-6328
Ivan V. Servetsky
Interregional Academy of Personnel Management, Educational and Scientific Institute of Law and Security named after Prince Volodymyr the Great
Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-5713-8911

INDICATORS OF THE USE OF ARTIFICIAL INTELLIGENCE IN INTELLIGENCE ACTIVITIES

Summary. *The article examines the indicators that demonstrate the use of artificial intelligence (AI) technologies in the activities of foreign intelligence services. It analyzes typical markers—both technical and behavioral, enabling the identification of large-scale analytics, automated data collection and classification, synthetic media, and AI-based decision-support systems. The research methodology combines a review of open-source intelligence (OSINT), comparative analysis of documented incidents, and the synthesis of external indicators (anonymized case studies, traffic patterns, and publication trends). The key categories of indicators are distinguished: the scale and speed of analytical outputs; the regularity and uniformity of messaging; the emergence of synthetic or transformed content (deepfakes, generative texts); adaptive behavioral models in contacts and campaigns; and cross-platform coordination of activities. The article addresses national security risks, as well as the ethical and legal dimensions of AI use in intelligence, and proposes general directions for monitoring and the development of counteraction policies.*

Keywords: *intelligence, artificial intelligence, services, OSINT, synthetic media, AI usage indicators, national security.*

Постановка проблеми. Швидкий розвиток і поширення технологій штучного інтелекту (ШІ) суттєво змінили інструментарій та підходи у сфері розвідувальної діяльності. Системи машинного навчання, великі мовні моделі, генеративні нейромережі й автоматизовані платформи для аналізу даних відкривають нові можливості для збору, обробки та маніпулювання інформацією: від масштабного використання відкритих джерел (OSINT) і аналізу розвідувальної інформації до створення синтетичних медіа (deepfake) та автоматизованих бот-мереж.

Водночас ці технології істотно ускладнюють традиційні підходи до виявлення, атрибуції та протидії розвідувальним операціям іноземних спецслужб. Проблема полягає в тому, що наявні індикатори та методики моніторингу часто не встигають за темпами інновацій у сфері ШІ: значна частина операцій маскується під природну інформаційну активність, штучно створений контент стає дедалі більш правдоподібним, а масштабні автоматизовані процеси стають менш помітними у звичайних каналах комунікації. Окрім технічних викликів, постає комплекс правових, етичних і організаційних проблем: відсутність чітких стандартів і процедур для виявлення та інформування працівників органів безпеки про використання ШІ у розвідувальній діяльності; недостатня інтеграція між кіберпідрозділами, службами безпеки й

аналітичними центрами; а також дефіцит кваліфікованих кадрів і ресурсів для постійного моніторингу інформаційного простору.

Недооцінка цих складнощів становить загрозу як для безпеки національних інтересів, так і для стійкості громадського суспільства. Неефективне виявлення та реагування на операції, створені з використанням штучного інтелекту, може спричинити дезінформацію, підірвати довіру до безпекових інституцій, сприяти маніпуляції суспільною думкою та скомпрометувати критично важливі рішення. Тому виникає потреба у систематизації ознак та індикаторів, що дозволяють достовірно й своєчасно ідентифікувати застосування штучного інтелекту саме в розвідувальній діяльності.

Метою статті є висвітлення та розробка практично орієнтованих рекомендацій щодо їх застосування у моніторингу, аналізі та впровадженні конкретних заходів протидії розвідувальній діяльності держав, які ведуть агресивну війну проти України. Для досягнення цієї мети дослідження поєднує огляд відкритих джерел (OSINT), аналіз задокументованих інцидентів і системний підхід до виокремлення техніко-поведінкових індикаторів ворожих спецслужб, що дозволяє дати відповіді на такі питання:

- Які ознаки найчастіше супроводжують використання ШІ у розвідувальних операціях іноземних спецслужб?
- Наскільки ці ознаки, що використовують організовані групи розвідувальній діяльност є небезпечними?
- Які методи збору та аналізу індикаторів є найефективнішими в умовах обмежених ресурсів і високої швидкості інформаційних потоків?
- Які організаційні та правові заходи можуть посилити спроможність державних інституцій виявляти та реагувати на такі загрози?

Очікуваним результатом є створення практично орієнтованої системи категорій ознак і рекомендацій, що підвищують спроможності національних структур своєчасно ідентифікувати та адекватно реагувати на використання ШІ у розвідувальній діяльності.

Аналіз останніх досліджень та публікацій. Дослідження останніх років засвідчують прискорення двох взаємопов’язаних процесів:

1. Активна інтеграція генеративних та аналітичних інструментів ШІ у робочі процеси державних і недержавних інституцій;
2. Паралельне зростання інструментів протидії (системи детекції, регуляторні політики, міжорганізаційна координація).

Отримані висновки узгоджуються з оглядом політик і стратегій НАТО, а також із аналітичними звітами приватних центрів дослідження ризиків.

Значне зростання кількості й якості синтетичного контенту (deepfakes, голосові підміни, генеративні тексти). Зафіксовано сотні випадків політично орієнтованих deepfake-матеріалів, а також зростання їх використання у фінансовому шахрайстві та рідвідувальній діяльтносмті. Використання LLM та генеративних інструментів у підготовці операцій (фаза розвідки, таргетинг, створення наративів, автоматизація фішингових і соціоінженерних атак). Ці технології вже застосовувалися у реальних кампаніях, які були перервані або виявлені платформами та постачальниками. Синергія між організованими групами та державними структурами (“proxy”-використання). Злочинні мережі дедалі частіше надають послуги, посилені ШІ, на користь ворожих держав.

Посилена увага політиків і міжнародних інституцій до регулювання та формування стратегій щодо застосування ШІ у сфері безпеки. Зокрема, відзначається оновлення стратегій НАТО та поява наукових і політичних рекомендацій від провідних аналітичних центрів. Recorded Future — “Targets, Objectives, and Emerging Tactics of

Political Deepfakes" (Insikt Group, 2024). Збірка інцидентів deepfake за певний період із аналізом тактик, цілей та каналів розповсюдження; корисна база кейсів для ідентифікації патернів. CSIS (2024). Аналітика щодо deepfakes та їх застосувань у зовнішній політиці: описано можливі сценарії використання, ризики для довіри та рекомендації щодо інституційної готовності.

Звіти провайдерів і приватних дослідницьких груп (Microsoft, OpenAI, Recorded Future, TRM Labs, Europol). Представлено реальні інциденти, приклади перерваних кампаній і перші техніки виявлення. Академічні статті (ACL, ACM та ін.) і політичні дослідження. Проаналізовано вплив ШІ-інтервенцій на сприйняття інформації, проведено експерименти з індикаторами достовірності та запропоновано методики валідації.

Виклад основного матеріалу. Аналітичні огляди міжнародних інституцій (NATO, Brookings тощо) свідчать про те, що стратегічні наслідки використання ШІ в розвідці тісно пов'язані з питаннями співробітництва та регулювання. Кейс-орієнтований OSINT (збір і класифікація конкретних інцидентів, формування timeline подій): дає практичні рекомендації, але вразливий до проблем підтвердження даних і упередженості вибірки. Мережевий і контент-аналіз (аналіз метаданих, поведінки ботів, сіток поширення): дозволяє виявляти автоматизацію та координацію інформаційних операцій.

Технічні методи детекції синтетичного контенту (моделі виявлення deepfake, лінгвістичні маркери для генеративних текстів). Хоча спостерігається прогрес, загальна точність у реальних умовах поки що залишається обмеженою. Сучасні розвідувальні служби активно впроваджують технології штучного інтелекту (ШІ) у різні напрями своєї діяльності: від інформаційно-психологічних операцій до кіберрозвідки, HUMINT (агентурна розвідка) та OSINT (розвідка з відкритих джерел) [1; 13].

Використання ШІ дозволяє розвідувальним органам ефективніше збирати, обробляти й аналізувати великі масиви даних, автоматизувати рутинні завдання, виявляти приховані закономірності та підтримувати процес ухвалення рішень у режимі, максимально наближеному до реального часу [1]. Подібна трансформація спостерігається як у західних спецслужбах, так і в країнах-антагоністах НАТО, що підтверджується стратегічними документами та аналітичними звітами [13; 1].

Одним із найпомітніших проявів використання штучного інтелекту є масовані приховані кампанії впливу, коли генеративні моделі застосовуються для автоматичного створення тисяч текстів, зображень або відео з подальшим швидким багатомовним розповсюдженням і повторенням єдиних шаблонів. Дослідження Graphika та інші кейси демонструють приклади мереж, що поширювали згенерований контент кількома мовами за спільними стилістичними патернами [11].

У звітах компаній Meta та Microsoft також зафіксовано діяльність мереж і кампаній, де використовувалися штучно згенеровані фотографії профілів, deepfake-відео та автоматизовані пости різними мовами. Окремі зразки таких операцій були виявлені та частково нейтралізовані платформами [4; 1; 5].

Характерні індикатори: однотипність повідомлень, повторювані мовні й візуальні шаблони, а також синхронна активація численних акаунтів, що дозволяють ідентифікувати подібні кампанії вже на ранніх етапах [11; 2].

Поява deepfake-відео та аудіозаписів є чітким індикатором використання генеративних технологій. Такі підробки часто містять технічні артефакти синтезу: розсинхронізацію руху губ і звуку, неприродну міміку, аномалії відблисків чи текстур шкіри, які дозволяють експертам ідентифікувати фальсифікацію [14; 2]. Відомі кейси

свідчать, що навіть якщо окремі deepfake-матеріали на перший погляд виглядають переконливо, детальний технічний аналіз зазвичай виявляє “підписи” штучного генерування (артефакти кадрування, аномалії голосу тощо) [14; 2].

Отже, підозрілі відео чи аудіозаписи із зображенням або голосом публічних осіб доцільно перевіряти насамперед на наявність цих технічних маркерів.

Штучний інтелект суттєво підвищує ефективність фішингу та соціальної інженерії: великі мовні моделі здатні генерувати переконливі, граматично бездоганні й персоналізовані повідомлення, що дає змогу запускати “автоматизовані конвеєри” атак, охоплюючи одночасно тисячі цілей [8; 12].

Аналітичні дослідження свідчать, що сучасні моделі дозволяють повністю автоматизувати цикл підготовки цілеспрямованих атак — від збору даних про жертву до створення індивідуалізованого листа. Це робить подібні операції дешевшими та масштабнішими [8; 12].

Відтак зникнення звичних “червоних прапорців” у повідомленнях (низька якість стилю, орфографічні помилки) стає ще одним важливим індикатором, який необхідно враховувати під час аналізу підозрілих листів. ШІ також використовується для створення та вдосконалення шкідливого програмного забезпечення: моделі здатні генерувати тисячі варіантів коду, змінюючи назви змінних, структуру або вставляючи “сміттєвий” код, що ускладнює сигнатурну детекцію та загострює протистояння між захисними й атакувальними системами [9; 3]. Аналітики відзначають певні ознаки машинного походження коду — надмірно акуратні коментарі, повторювані фразеологічні патерни, раптові множинні варіації одного зразка — які можуть слугувати сигналами для детальнішого розслідування [3; 9].

У сфері OSINT розвідки штучний інтелект дає змогу автоматизувати переклади, семантичний пошук, тональний аналіз і швидко опрацьовувати великі масиви текстової та медійної інформації, що дозволяє “просіювати” релевантні дані в масштабах, недосяжних для суто людських команд [1; 10]. Аналогічно, у SIGINT алгоритми автоматичної транскрипції й перекладу роблять перехоплення “пошуковими”, відкриваючи можливість відбирати та фільтрувати сотні чи навіть тисячі годин аудіопотоку за ключовими словами чи голосами [1; 13]. Таким чином, раптове зростання можливостей аналітики в обробці багатомовного контенту може слугувати непрямою ознакою застосування ШІ-інструментів.

У сфері HUMINT штучний інтелект використовується для високоточного відбору потенційних об’єктів вербування, створення синтетичних цифрових особистостей у соцмережах та застосування deepfake-голосів для безпосереднього контакту. Дослідження Stanford Internet Observatory та інші аналітичні огляди виявили масиви фейкових профілів із AI-згенерованими фотографіями, які використовуються для встановлення довіри та розвідки намірів цілей [10; 11]. Це свідчить, що поява добре оформлених, але не верифікованих профілів, а також раптові звернення від “рекрутерів” можуть бути індикаторами агентурної операції, підсиленої технологіями ШІ.Матеріально-технічні сліди також можуть бути індикаторами: закупівлі великих GPU-кластерів через компанії-прокладки, реекспорт серверів чи розгортання короткострокових обчислювальних “ферм” для інференсу здатні свідчити про підготовку до масштабного застосування генеративних моделей [6].

Журналістські розслідування фіксують випадки реекспорту високопродуктивних GPU до країн, що перебувають під санкціями, — це непряма, проте вагома ознака розгортання AI-потужностей [6]. Крім того, аналіз аномалій у споживанні електроенергії

або раптові сплески хмарних обчислювальних запитів можуть виступати індикаторами тимчасових AI-кампаній.

Враховуючи викладене та відповідаючи на поставлене питання щодо найпоширеніших ознак застосування ШІ, можна виокремити такі технічні індикатори: мовні "галюцинації" (вигадані факти, недоречні вставки), шаблонність формулювань у текстах, повторювані стилістичні помилки, а також водяні знаки чи артефакти в зображеннях і відео. Дослідження з маркування/водяних знаків і їхніх обмежень засвідчують, що хоча деякі моделі вбудовують стеганографічні підписи, ці підходи наразі не є універсальним рішенням і можуть бути зламані або обійдені [15; 14].

Крім того, мережеві індикатори — зокрема, нетипові TLS-сесії чи регулярні звернення до API відомих AI-сервісів у поведінці підозрілих акаунтів — можуть виступати непрямим підтвердженням використання зовнішніх генеративних платформ [7; 1].

Висновки. Сучасні технології штучного інтелекту істотно змінюють інструментарій розвідувальних спецслужб іноземних держав, роблячи їхні операції більш масштабними, швидкими та технічно замаскованими. Штучний інтелект стрімко інтегрується у практику розвідувальних операцій, залишаючи після себе цілий комплекс слідів: від мовних і візуальних артефактів у контенті до матеріальних (GPU-поставки) та мережевих (запити до AI-API) індикаторів.

Ознаки використання ШІ спецслужбами простежуються в інформаційних операціях, кіберзагрозах, аналізі відкритих даних і навіть у HUMINT. Їх виявлення можливе через аналіз контенту, телеметрії, закупівельної діяльності та інфраструктурних слідів. Комбінація цих маркерів дає змогу контррозвідці та аналітикам ефективніше виявляти й документувати операції, підтримувані ШІ. Для перевірки й підтвердження кожного з таких індикаторів доцільно звертатися до джерел. Технічні (автоматизований збір даних, генеративні моделі, аналітичні пайплайни) й поведінкові (однотипність повідомлень, синхронізована активація мереж, адаптивні шаблони взаємодії) маркери у сукупності формують практично застосовні індикатори використання ШІ.

Водночас поодинокі технічні ознаки (наприклад, лише лінгвістичні аномалії чи лише нетипова швидкість публікацій) не є достатніми для достовірної ідентифікації. Найбільш надійні результати забезпечує комбінований підхід — поєднання техніко-поведінкових індикаторів, мережевого аналізу та контекстної валідації. При цьому існують значні виклики в атрибуції і верифікації операцій, зокрема через використання proxy-акторів (комерційні або кримінальні посередники) та обмеженість відкритих корпусів інцидентів. Це підриває можливість кількісної оцінки масштабів і ефективності аналізу використання ШІ.

Правові, етичні та організаційні бар'єри уповільнюють реагування на виклики, що створює ШІ: відсутність уніфікованих процедур обміну даними між платформами, державними органами та дослідницькими центрами, а також дефіцит кваліфікованих кадрів і ресурсів знижують ефективність оперативної детекції й розслідування. Практична готовність державних інститутів визначається не лише наявністю технологій детекції, а й процедурною спроможністю — тобто забезпеченням швидкого оповіщення, міжсекторальної координації та чітких правових рамок для реагування.

Аналітичні дослідження підтверджують потребу у переході від демонстраційних методик до системних рішень: стандартизовані індикатори, відкриті де-майндовані корпуси інцидентів, регулярні польові випробування інструментів детекції й узгоджені метрики для оцінки впливу ШІ.

Наразі необхідно впроваджувати гібридну систему індикаторів, яка поєднує технічні, мережеві та контентні ознаки, а також формалізувати порогові правила для запуску розслідувань. Також важливо розвивати механізми обміну інформацією між державними структурами, платформами та приватними аналітичними центрами із забезпеченням правових гарантій і процедур захисту даних. Усе це свідчить про докорінні зміни в підготовці аналітиків (тренінги з OSINT, розпізнавання синтетичного контенту, мережевий аналіз) та створення мультидисциплінарних команд, які об'єднують технічних спеціалістів, аналітиків і юристів.

Необхідно розробити національні й міжнародні правила та процедури реагування на виявлені кампанії з урахуванням правових та етичних аспектів, а також сценаріїв для критичних періодів (вибори, кризові події). Разом з тим такі дослідження обмежене доступністю відкритих даних і зосереджене на публічно зареєстрованих кейсах; це може недооцінювати приховані чи ретельно замасковані операції. Подальші ефективні дослідження мають включати longitudinal-аналітику, експериментальну перевірку гібридних індикаторів у реальних умовах та глибинне вивчення механік proxy-взаємодій між державними та кримінальними акторами.

Отже, систематизація ознак і впровадження оперативних процедур їх застосування суттєво підвищить здатність національних інституцій виявляти та протидіяти інструменталізації ШІ у розвідувальний діяльності.

ПОДЯКИ: Немає

КОНФЛІКТ ІНТЕРЕСІВ: Немає

Список використаних джерел:

1. Microsoft Corporation. (2024). *Microsoft Digital Defense Report 2024*. Retrieved September 22, 2025, from https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf

2. Recorded Future (Insikt Group). (2024, September 24). *Targets, Objectives, and Emerging Tactics of Political Deepfakes*. Retrieved September 22, 2025, from https://go.recordedfuture.com/hubfs/reports/ta-2024-0924.pdf

3. Palo Alto Networks (Unit 42). (2025). *2025 Unit 42 Global Incident Response Report: Social engineering edition*. Retrieved September 22, 2025, from https://unit42.paloaltonetworks.com/2025-unit-42-global-incident-response-report-social-engineering-edition/

4. Meta. (2024, October 11). *Taking action against coordinated inauthentic behavior in Moldova*. Meta Newsroom. Retrieved September 22, 2025, from https://about.fb.com/news/2024/10/taking-action-against-coordinated-inauthentic-behavior-in-moldova/

5. Hern, A. (2024, December 3). Meta says it has taken down about 20 covert influence operations in 2024. *The Guardian*. Retrieved September 22, 2025, from https://www.theguardian.com/technology/2024/dec/03/meta-says-it-has-taken-down-about-20-covert-influence-operations-in-2024

6. Seddon, M. (2024, October 27). How a Mumbai drugmaker is helping Putin get Nvidia AI chips. *Bloomberg*. Retrieved September 22, 2025, from https://www.bloomberg.com/news/features/2024-10-27/russia-is-getting-nvidia-ai-chips-from-an-indian-pharma-company

7. Reuters. (2024, May 30). OpenAI has stopped five attempts to misuse its AI for 'deceptive activity'. Retrieved September 22, 2025, from

https://www.reuters.com/technology/cybersecurity/openai-has-stopped-five-attempts-misuse-its-ai-deceptive-activity-2024-05-30/

8. Heiding, F. (2024, May 30). *AI Will Increase the Quantity — and Quality — of Phishing Scams*. *Harvard Business Review*. Retrieved September 22, 2025, from https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams

9. Lakshmanan, R. (2024, December 23). AI Could Generate 10,000 Malware Variants, Evading Detection in 88% of Case. *The Hacker News*. Retrieved September 22, 2025, from https://thehackernews.com/2024/12/ai-could-generate-10000-malware.html

10. Stanford Internet Observatory. (2024, March 18). *How Spammers, Scammers and Creators Leverage AI to Build Followers / AI spam accounts build followers*. Retrieved September 22, 2025, from https://cyber.fsi.stanford.edu/news/ai-spam-accounts-build-followers

11. Graphika. (2024, October 11). *China and the 2024 Election: Graphika insights*. Retrieved September 22, 2025, from https://graphika.com/posts/china-and-the-2024-election-graphika-insights-featured-by-washington-post

12. Hazell, J. (2023). *Spear Phishing With Large Language Models* (arXiv:2305.06972). Retrieved September 22, 2025, from https://arxiv.org/pdf/2305.06972.pdf

13. NATO. (2024, July 10). *Summary of NATO's revised Artificial Intelligence (AI) strategy*. Retrieved September 22, 2025, from https://www.nato.int/cps/en/natohq/official_texts_227237.htm

14. Feizi, S., et al. (2023, October 3). Researchers Tested AI Watermarks—and Broke All of Them. *Wired*. Retrieved September 22, 2025, from https://www.wired.com/story/artificial-intelligence-watermarking-issues

15. Tancik, M., Mildenhall, B., & Ng, R. (2020). *StegaStamp: Invisible Hyperlinks in Physical Photographs* (CVPR 2020 paper). Retrieved September 22, 2025, from https://openaccess.thecvf.com/content_CVPR_2020/papers/Tancik_StegaStamp_Invisible_Hyperlinks_in_Physical_Photographs_CVPR_2020_paper.pdf

Олександр Володимирович Сушко
аспірант Міжрегіональної академії управління персоналом, Науково-навчальний інститут права та безпеки імені князя Володимира Великого
03138, Україна, м. Київ, пров. Мостовий, буд 13
юрист у компаніях - АО ЮФ Робінсон Патман, ТОВ АПОГЕЙ
email: asushkoolek@gmail.com

Іван Васильович Сервецький,
доктор юридичних наук
Заступник завідувача кафедри національної безпеки. Професор кафедри Національної безпеки, Науково-навчальний Інститут права та безпеки імені князя Володимира Великого Міжрегіональної академії управління персоналом
03039, Україна, м. Київ, вул. Фрометівська, 2.
email: Siv2055@gmail.com

Oleksandr V. Sushko
Lawyer at law firms – AO “LF Robinson Patman”, LLC “APOGEY”
PhD Student
Interregional Academy of Personnel Management (IAPM), Educational and Scientific Institute of Law and Security named after Prince Volodymyr the Great
13 Mostovyi Lane, Kyiv, 03138, Ukraine
email: asushkoolek@gmail.com

Ivan V. Servetsky
Doctor of Law
Deputy Head of the Department of National Security, Professor of the Department of National Security, Interregional Academy of Personnel Management (IAPM), Educational and Scientific Institute of Law and Security named after Prince Volodymyr the Great
2 Frometivska St., Kyiv, 03039, Ukraine
email: Siv2055@gmail.com

Рекомендоване цитування: Сушко О.В., Сервецький І.В. Ознаки використання штучного інтелекту у розвідувальній діяльності. *Інформація і право.* № 1(56)/2026. 2026. С. 137-145. https://doi.org/10.37750/2616-6798.2026.1(56).357368.

Suggested Citation: Sushko O., Servetsky I. (2026) Indicators of the Use of Artificial Intelligence in Intelligence Activities. *Information and Law*. 1(56)/2026. 137-145. https://doi.org/10.37750/2616-6798.2026.1(56).357368.

Дата надходження статті до редакції: 25.02.2025 р.
Дата прийняття статті до друку після рецензування: 02.03.2026 р.
Дата публікації (оприлюднення): 01.04.2026 р.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~