Технічні науки

УДК 004.056:004.738.5

Петровський Денис Тарасович

здобувач першого (бакалаврського) рівня вищої освіти

Львівського державного університету внутрішніх справ

Petrovskyi Denys

Applicant for the First (Bachelor's) Level of Higher Education

Lviv State University of Internal Affairs

Огірко Ольга Ігорівна

кандидат технічних наук, доцент,

професор кафедри інформаційних технологій

Львівський державний університет внутрішніх справ

Ohirko Olha

PhD in Technical Sciences, Associate Professor,

Professor of the Department of Information Technologies

Lviv State University of Internal Affairs

DOI: https://doi.org/10.25313/2520-2057-2026-6-12073

ВИКОРИСТАННЯ OSINT У СИСТЕМІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ
USE OF OSINT IN THE SYSTEM OF INFORMATION AND ANALYTICAL SUPPORT

Анотація. *У статті досліджено особливості використання OSINT у системі інформаційно-аналітичного забезпечення в умовах сучасних кіберзагроз та інформаційної війни. Проаналізовано основні джерела відкритої інформації, напрями OSINT-розвідки (GeoINT, SOCMINT,*

TECHINT), а також їх значення для національної безпеки, правоохоронної діяльності та кібербезпеки. Окрему увагу приділено правовим та етичним аспектам обробки інформації й захисту персональних даних.

Ключові слова: *OSINT, відкриті джерела інформації, інформаційно-аналітичне забезпечення, кібербезпека, GeoINT, SOCMINT, GDPR, інформаційна війна, національна безпека, цифрові докази.*

Summary. *The article examines the peculiarities of using OSINT in the system of information and analytical support under conditions of modern cyber threats and information warfare. The main sources of open information, the key areas of OSINT intelligence (GeoINT, SOCMINT, TECHINT), as well as their importance for national security, law enforcement activities, and cybersecurity are analyzed. Particular attention is paid to the legal and ethical aspects of information processing and personal data protection.*

Key words: *OSINT, open source intelligence, information and analytical support, cybersecurity, GeoINT, SOCMINT, GDPR, information warfare, national security, digital evidence.*

У сучасних умовах повномасштабної збройної агресії російської федерації проти України, посилення гібридних загроз та інтенсивної цифрової трансформації суспільства особливого значення набуває розвідка з відкритих джерел інформації (Open Source Intelligence – OSINT). Цей інструмент перетворився на ключову складову системи інформаційно-аналітичного забезпечення державних органів, правоохоронних структур, журналістських та громадських організацій. Як обґрунтовано стверджують С. В. Легомінова, Ю. В. Щавінський, Д. І. Рабчун, М. М. Запорожченко та О. В. Будзинський у фаховому виданні «Кібербезпека: освіта, наука, техніка», «у сучасному цифровому просторі, де значні об'єми інформації стають доступними у відкритому доступі, інструменти OSINT надають

широкий спектр можливостей для отримання даних щодо фізичних та юридичних осіб з різних відкритих джерел» [1, с. 295]. Належне правове регулювання та системне використання OSINT набуває стратегічного значення для забезпечення національної безпеки України.

Поняття OSINT у сучасній науковій доктрині розкривається через здатність здобувати розвідувальну інформацію з усіх легально доступних джерел. Як справедливо зазначає М. О. Думчиков у фаховому виданні «Аналітично-порівняльне правознавство», «сьогодні в рамках OSINT можна здобути розвідувальні відомості з усіх відкритих джерел санкціонованим способом. До них належать інтернет-ресурси, медіа, державні реєстри та бази даних, комерційні й наукові публікації. Варто зауважити, що 90% усієї розвідувальної інформації можна отримати саме з відкритих джерел» [2, с. 275]. Цей факт принципово змінює парадигму інформаційно-аналітичної діяльності: основна цінність аналітика тепер полягає не у здобутті закритої інформації, а у здатності ефективно опрацьовувати колосальні обсяги відкритих даних, верифікувати їх та синтезувати в аналітичний продукт.

Багатоманітність відкритих джерел інформації, що використовуються в OSINT, чітко класифікована у науковій літературі. С. В. Легомінова та співавтори виділяють такі основні групи відкритих джерел: «традиційні ЗМІ (газети, радіо, телебачення, журнали); все, що публікується в інтернеті (соціальні мережі, блоги, форуми, онлайн-бази даних, в яких можна знайти особисті думки, враження, неформальні обговорення та іншу інформацію про окремих осіб чи організації); корпоративні дані, доступні для громадськості (фінансові звіти або інша інформація про організацію); урядова інформація (судові справи, публічні слухання, публічні документи); конференції та семінари, наукові статті, журнали, тези, дисертації, дослідження; фотографії; геопросторова інформація (картографічні дані, координати та інші параметри, що додають просторовий контекст до

зібраної інформації)» [1, с. 295–296]. Така диверсифікація джерел вимагає системного підходу до інформаційно-аналітичної діяльності.

У сучасній науковій літературі сформувалася стійка класифікація напрямів OSINT за типом джерел даних. М. О. Думчиков виокремлює такі ключові напрями: GeoINT (геопросторова розвідка) – «використовує супутникові знімки, картографічні сервіси та відкриті GPS-трекери для верифікації місця та часу подій. Завдяки GeoINT стало можливим відстеження переміщення військ та документування пошкоджень інфраструктури під час повномасштабного вторгнення Росії в Україну»; SOCMINT (розвідка соціальних медіа) – «фокусується на аналізі публікацій у соціальних мережах, таких як Facebook, X-Twitter, Telegram-канали та форуми. SOCMINT використовується для моніторингу розповсюдження ворожих наративів та ідентифікації ключових поширювачів»; TECHINT (технічна розвідка) – «охоплює аналіз інфраструктурних слідів: перевірка доменних реєстрів WHOIS для атрибуції джерел дезінформації, аналіз метаданих зображень»; та елементи HUMINT [2, с. 275]. Така класифікація дозволяє структурувати інформаційно-аналітичну діяльність за конкретними завданнями.

Особливу роль OSINT відіграє у системі інформаційно-аналітичного забезпечення правоохоронної діяльності. Як обґрунтовано стверджують К. Борисова, К. Жмуровська, Є. Кришталь та О. Деревягін у науковій статті, опублікованій у виданні «UNIVERSUM», «OSINT виступає не лише як допоміжний інструмент збору даних, а як повноцінна аналітична складова кримінальної розвідки, що забезпечує отримання, обробку та оцінку відомостей, релевантних до оперативних завдань. Застосування відкритих джерел дозволяє оперативним підрозділам здійснювати моніторинг медіа-простору, соціальних мереж і цифрових платформ, виявляти інформаційно-психологічні операції (ІПСО), встановлювати взаємозв'язки між суб'єктами» [3, с. 207]. Правовою основою такої діяльності виступає Закон

України «Про оперативно-розшукову діяльність» від 18.02.1992 № 2135-XII [4] та Закон України «Про національну безпеку України» від 21.06.2018 № 2469-VIII [5], які визначають повноваження уповноважених органів щодо здобуття інформації, у тому числі з відкритих джерел.

Використання OSINT у системі інформаційно-аналітичного забезпечення нерозривно пов'язане з необхідністю дотримання правових та етичних меж, особливо у сфері захисту персональних даних. Як справедливо акцентує М. О. Думчиков, OSINT «оперує на стику фундаментальних прав, зокрема права кожного на вільне збирання, зберігання та використання інформації й права на приватність» [2, с. 276]. Загальний регламент ЄС про захист даних (GDPR) встановлює найвищі глобальні стандарти для обробки персональних даних. Дослідник звертає увагу: «з погляду GDPR, для OSINT-розслідувань слід з обережністю використовувати згоду суб'єкта як правову підставу для обробки, оскільки існує високий ризик її оскарження або відкликання. Водночас більш надійною підставою є законний інтерес, за умови, що інтерес розслідування переважає над правом особи на приватність» [2, с. 276]. Це вимагає чіткої правової регламентації OSINT-діяльності в Україні.

Водночас використання OSINT створює і нові виклики для системи інформаційно-аналітичного забезпечення. С. В. Легомінова та співавтори обґрунтовано наголошують, що «не існує універсального інструменту для захисту від збору даних про організацію, проте існують превентивні заходи, які дозволяють пом'якшити наслідки інцидентів: вдосконалення внутрішніх комунікацій щодо ІБ, навчання та підвищення обізнаності персоналу для обмеження оприлюднення чутливої інформації; проведення OSINT-моніторингу для отримання чіткого розуміння того, яка інформація щодо організації може перебувати в розпорядженні потенційних атакуючих; впровадження сегментації мережі, ефективного управління правами користувачів та інших програмно-апаратних заходів безпеки» [1, с. 300]. Ці

заходи мають бути системно імплементовані як у державних, так і в приватних структурах.

Підсумовуючи викладене, варто зазначити, що OSINT перетворився на повноцінну та незамінну складову системи інформаційно-аналітичного забезпечення в умовах сучасних гібридних загроз. Водночас, як справедливо акцентує М. О. Думчиков, для забезпечення стійкості та легітимності OSINT у довгостроковій перспективі необхідно подолати два ключові виклики: «методологічна прозорість: в умовах зростання загрози deepfakes та маніпуляцій GenAI верифікація даних вимагає запровадження уніфікованих, прозорих і криміналістично сумісних стандартів» та «правова легітимізація: OSINT-розслідування мають чітко відповідати вимогам захисту персональних даних, покладаючись на законний інтерес як правову підставу та мінімізуючи збір надлишкової інформації» [2, с. 277]. Подальше вдосконалення системи має йти у напрямах: гармонізації національного законодавства з GDPR; розробки спеціалізованих стандартів верифікації OSINT-доказів для судового процесу; формування професійної підготовки OSINT-аналітиків; запровадження обов'язкових етичних кодексів. Лише комплексний підхід забезпечить ефективне використання OSINT у системі національної безпеки України.

Література

1. Легомінова С. В., Щавінський Ю. В., Рабчун Д. І., Запорожченко М. М., Будзинський О. В. Небезпека інструментів OSINT та способи пом'якшення наслідків їх використання для організації. *Кібербезпека: освіта, наука, техніка.* 2024. № 1(25). С. 294–303. DOI: https://doi.org/10.28925/2663-4023.2024.25.294303

2. Думчиков М. О. Відкрита розвідка (OSINT) у протидії інформаційним війнам: аналітичні інструменти та правові межі.

Аналітично-порівняльне правознавство. 2025. Вип. 6, ч. 2. С. 273–277. DOI: https://doi.org/10.24144/2788-6018.2025.06.2.43

3. Борисова К., Жмуровська К., Кришталь Є., Деревягін О. OSINT у правоохоронній діяльності: міжнародний досвід та українські перспективи. *UNIVERSUM*. 2025. № 25. С. 205–210. URL: https://archive.liga.science/index.php/universum/article/view/2155 (дата звернення: 28.04.2026).

4. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12 (дата звернення: 28.04.2026).

5. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 28.04.2026).