МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ УНІВЕРСИТЕТ

МІЖНАРОДНА КОНФЕРЕНЦІЯ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

(ПТІКІ'2026)

Одеса, Україна, 16 липня 2026 р.

Матеріали конференції

ОДЕСА

2026

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ УНІВЕРСИТЕТ

МІЖНАРОДНА КОНФЕРЕНЦІЯ

«Передові технології в інформаційно-комунікаційній інженерії»

(ПТІКІ'2026)

Одеса, Україна, 16 липня 2026 р.

Матеріали конференції

Одеса

2026

УДК 004.9
ББК 32

Проведення заходу зареєстровано в Державній науковій установі «Український інститут науково-технічної експертизи та інформації» (Реєстраційний номер: 3326U000765 від 01-07-2026 р.).

Рецензенти:
Надія КАЗАКОВА – д.т.н., професор, завідувач кафедри інформаційних технологій Одеського національного університету ім. І.І. Мечнікова
Віктор СТРЕЛЬБИЦЬКИЙ – к.т.н., доцент, доцент кафедри підйомно-транспортні машини та інжиніринг портового технологічного обладнання Одеського національного морського університету

International Conference "Advanced Technology in Information and Communication Engineering" (ATICE'2026): Conference Proceedings. Odesa: International university, 2026, 145 p**.**
DOI: https://doi.org/10.32837/11300.33747

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2026): Матеріали конференції. Одеса: Міжнародний університет, 2026, 145 с.

У збірнику подано результати наукових досліджень, висвітлено обговорення актуальних проблем, викликів і тенденцій з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами у різних галузях народного господарства. Матеріали охоплюють інноваційні підходи, досвід упровадження сучасних рішень і приклади успішних практик трансформації різних галузях народного господарства .

Видання призначене для науково-педагогічних працівників, здобувачів освіти, науковців і фахівців ІТ галузі.

Відповідальні за випуск:
к.т.н., доцент Пунченко Наталія,
к.т.н., доцент Розенвассер Денис.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова

КІВАЛОВ С.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.

Співголови

ГРОМОВЕНКО К.В. – д.ю.н., проф., Міжнародний університет, м. Одеса, Україна.
ЛЕФТЕРОВ В.О. – д.п.н., проф., Міжнародний університет, Одеса, Україна
СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, Одеса, Україна.
УРИВСЬКИЙ Л.О. – д.т.н., проф., НТУ України "КПІ імені Ігоря Сікорського", Київ, Україна.

Члени організаційного комітету

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ЙОНА Л.Г. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
РУСУ О.П. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ВАКАРЧУК А.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ПУНЧЕНКО Н.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ГРІБОВА В.В. – к.ф.-м.н., доц., Міжнародний університет, Одеса, Україна.

РЕДАКЦІЙНИЙ КОМІТЕТ

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ПУНЧЕНКО Н.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.

КОМІТЕТ МІЖНАРОДНИХ ЗВ'ЯЗКІВ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
ГЛОБА Л. С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ВЧЕНИЙ СЕКРЕТАР

ПУНЧЕНКО Н.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ЗМІСТ

УДК 004.056

DOI: https://doi.org/10.32837/11300.33763

OSINT У КІБЕРБЕЗПЕЦІ

Розенвассер Д.М.
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій
Міжнародний університет
м. Одеса, Україна
Шведу М.І.
здобувачка 3-го курсу першого (бакалаврського) рівня
зі спеціальності 125 Кібербезпека та захист інформації
Міжнародний університет
м. Одеса, Україна

Анотація. *У роботі розглянуто особливості використання технологій OSINT (Open Source Intelligence) у сфері кібербезпеки. Проаналізовано основні джерела відкритої інформації, сучасні інструменти збору даних, методи їх аналізу та можливості практичного застосування під час виявлення кіберзагроз. Особливу увагу приділено оцінці ефективності OSINT-аналізу, використанню спеціалізованих програмних засобів, а також ролі відкритої розвідки у попередженні кіберінцидентів.*

Стрімкий розвиток інформаційних технологій призвів до безпрецедентного збільшення обсягів відкритої інформації, що щоденно публікується в мережі Інтернет. Соціальні мережі, офіційні вебресурси, державні реєстри, спеціалізовані форуми, картографічні сервіси та інші відкриті джерела містять величезний масив даних, який може використовуватися як для законної аналітичної діяльності, так і під час здійснення кіберзлочинів [1-4].

У сфері кібербезпеки своєчасне отримання достовірної інформації дозволяє значно скоротити час реагування на потенційні загрози, оцінити рівень ризику та своєчасно виявити можливі вразливості інформаційних систем. Саме тому технології OSINT сьогодні є одним із найбільш актуальних і перспективних напрямів цифрової розвідки [5-6].

Метою роботи є дослідження можливостей використання OSINT у кібербезпеці, аналіз сучасних інструментів відкритої розвідки та оцінка їх ефективності при забезпеченні інформаційної безпеки.

На відміну від традиційної розвідки, процес пошуку, збору, обробки та аналізу інформації, отриманої виключно із законних відкритих джерел (OSINT) не передбачає несанкціонованого доступу до інформації чи використання спеціальних технічних засобів проникнення [2-4].

Процес OSINT включає декілька етапів:

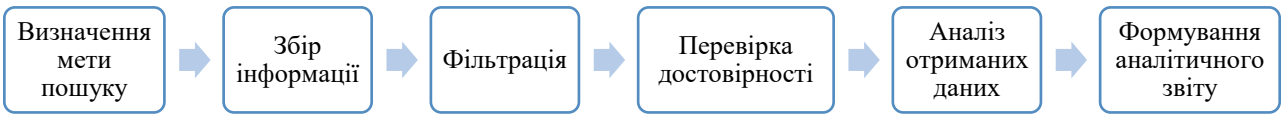

Рисунок 1 – Етапи відкритої розвідки

У сучасній кібербезпеці OSINT використовується практично на всіх етапах забезпечення захисту інформаційних систем.

Під час проведення аудиту інформаційної безпеки OSINT дозволяє ще до початку активного тестування знайти значну кількість потенційних проблем. Крім того, відкрита розвідка широко використовується під час реагування на кіберінциденти (Incident Response), цифрової криміналістики (Digital Forensics) та аналітиці загроз (Threat Intelligence) [5-6].

Ефективність застосування OSINT залежить від якості вихідних даних та правильності їх аналізу. На відміну від автоматизованого сканування мережі, відкрита розвідка дозволяє отримати значно ширший контекст щодо діяльності організації [2-6].

Рисунок 2 – Основні складові OSINT-дослідження

Разом із перевагами існують і певні недоліки. Частина інформації може бути застарілою або навмисно неправдивою. Саме тому одним із головних принципів OSINT є перевірка отриманих відомостей із декількох незалежних джерел [2, 4, 7].

Для кількісного оцінювання показника ефективності застосування відкритої розвідки можна використати інтегральну модель розрахунку:

$$E_{OSINT} = w_1 D + w_2 R + w_3 C + w_4 T$$

де D – повнота інформації (Completeness);
R – достовірність інформації (Reliability);
C – актуальність інформації (Currency);
T – оперативність отримання інформації (Timeliness);
w_i – вагові коефіцієнти, при цьому:

$$\sum_{i=1}^{4} w_i = 1$$

Найбільш поширені інструменти відкритої розвідки наведено в таблиці 1 [8]:

Таблиця 1 – Порівняльний аналіз сучасних OSINT-інструментів

Інструмент	Основне призначення	Переваги	Недоліки
Maltego	Аналіз взаємозв'язків	Потужна візуалізація	Частина функцій платна
Shodan	Пошук пристроїв Internet	Велика база IoT	Не всі функції актуальні
Spider Foot	Автоматичний збір даних	Автоматизовано	Тривале сканування
theHarvest	Збір e-mail доменів	Простота використання	Менша функціональність
Censys	Аналіз мережевих реєстрів	Глибокий пошук	Необхідна реєстрація

Застосування декількох інструментів одночасно значно підвищує повноту та достовірність отриманої інформації. Одним із найбільш поширених прикладів використання OSINT є аудит цифрового сліду [3, 4, 9].

Отримані результати дозволяють фахівцям своєчасно виявити та усунути потенційні вразливості ще до того, як ними скористаються зловмисники.

Висновки. Використання відкритих джерел інформації дозволяє значно підвищити ефективність аналізу кіберзагроз, своєчасно виявляти потенційні ризики та приймати обґрунтовані рішення щодо захисту інформаційних систем.

Інтеграція методів відкритої розвідки в діяльність фахівців із кібербезпеки забезпечує можливість комплексного дослідження цифрового середовища без порушення законодавства. Подальший розвиток технологій штучного інтелекту, машинного навчання та автоматизованих систем аналізу даних сприятиме підвищенню точності й швидкості OSINT-досліджень, що робить цей напрям одним із найперспективніших у сфері інформаційної безпеки.

Література

1. Bennett W. L., Livingston S. The disinformation order: Disruptive communication and the decline of democratic institutions // *European Journal of Communication*. 2018. Vol. 33, No. 2. P. 122–139. DOI: 10.1177/0267323118760317.
2. Hwang Y.-W., Lee I.-Y., Kim H., Lee H., Kim D. Current Status and Security Trend of OSINT // *Wireless Communications and Mobile Computing*. 2022. Article ID 1290129. DOI: 10.1155/2022/1290129.
3. Layton R., Watters P. A. Automating Open Source Intelligence: Algorithms for OSINT. Elsevier, 2016. 211 p.
4. Lande D. V., Shnurko-Tabakova E. OSINT as a part of cyber defense system // *Theoretical and Applied Cybersecurity*. 2019. Vol. 1, No. 1. P. 103–108. DOI: 10.20535/tacs.2664-29132019.1.169091.
5. Користін О. OSINT Open Source Intelligence. Теорія та методологія: монографія / Користін О., Демедюк С., Барановський О., Ланде Д. та ін. за заг.ред. Користіна О.Є., Демедюка С.В. Київ: 7БЦ, 2025. 304 с.
6. Користін О. 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.
7. Rajamäki J., McMenamin S., Tiitta K. Utilization and Sharing of Cyber Threat Intelligence Produced by Open-Source Intelligence // *Proceedings of the 19th International Conference on Cyber Warfare and Security (ICCWS)*. 2024. DOI: 10.34190/ICCWS.19.1.2069.
8. Мірошніченко, І. О. Роль методів OSINT в кібербезпеці та їх застосування під час воєнних конфліктів / І. О. Мірошніченко, Д. В. Ланде // Теоретичні і прикладні проблеми фізики, математики та інформатики: матеріали XXII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених, [Київ], 13−17 травня 2024 р. / КПІ ім. Ігоря Сікорського. Київ, 2024. С. 282-284.
9. Browne T. O., Abedin M., Chowdhury M. J. M. A Systematic Review on Research Utilising Artificial Intelligence for Open Source Intelligence (OSINT) Applications // *International Journal of Information Security*. 2024. Vol. 23, No. 4. P. 2911–2938. DOI: 10.1007/s10207-024-00868-2.