НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

UDC 004.056

Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

ВИКОРИСТАННЯ OPENDATA UKRAINE В ЦІЛЯХ OSINT

Бойко Віктор

кандидат технічних наук, доцент кафедри кібербезпеки
Національного університету «Одеська юридична академія»

Дручик Софія

студентка 4-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

У сучасному світі інформація є стратегічним ресурсом, який може визначати економічний, політичний та навіть військовий успіх держав і організацій. Одним із найважливіших напрямів роботи з інформацією є OSINT (Open Source Intelligence) – розвідка з відкритих джерел. Цей підхід дозволяє отримувати, аналізувати та інтерпретувати дані, які є у відкритому доступі, без використання засекречених або спеціальних каналів.

OpenData – це інформація, що генерується державою та оприлюднюється в машиночитаній формі для її подальшого використання бізнесом, громадськістю, журналістами, дослідниками та органами влади [1]. Відкриті дані – це в першу чергу можливість легкого, ефективного та стандартизованого обміну даними між усіма зацікавленими сторонами, в тому числі самими органами влади. Це дієвий механізм, який не лише “змушує” ділитися інформацією, але й допомагає отримувати дивіденди від цього. Основними ознаками інформації з відкритих джерел є те, що для її отримання не потрібно використовувати будь-які методи таємного збору, і що вона повинна бути отримана за допомогою засобів, які повністю відповідають авторським правам і комерційним вимогам постачальників, де це можливо". В Україні ключовою платформою є портал відкритих даних data.gov.ua, створений у рамках закону «Про доступ до публічної інформації». Він об’єднує тисячі наборів даних від різних органів державної влади та місцевого самоврядування [2].

OSINT (Open Source Intelligence) – це розвідка, заснована на аналізі відкритих джерел. Тобто всього, що є у вільному доступі: соціальні мережі, форуми, ЗМІ, державні реєстри, супутникові знімки, відео, бази злитих даних тощо. Простими словами – OSINT дозволяє знайти про людину або організацію максимум даних, не порушуючи закону. Це своєрідна легальна “розвідка”, але побудована не на хакерстві, а на аналітичному мисленні, досвіді і знанні джерел [3]. OSINT в основному використовується у функціях національної безпеки, правоохоронних органів та бізнес-розвідки, а також має цінність для аналітиків, які використовують неконфіденційні розвідувальні дані, що відповідають на секретні, несекретні або власні розвідувальні запити в рамках попередніх розвідувальних дисциплін [4].

У кібербезпеці OSINT може використовуватись як для захисту, так і для нападу. Ці техніки можуть допомогти у виявленні витоку даних. Часто хакери після зламу систем публікують частину вкрадених даних у згаданому вже даркнеті, щоб продемонструвати «товар». Якщо компанія вчасно зреагує, вона може запобігти подальшому розповсюдженню і зберегти недоторканність чутливих даних, які не входили до «демонстраційного пакету» [5].

Про відкриті дані в Україні всерйоз заговорили на початку 2013 року. Однією з перших ініціатив став проект Social Boost, що просуває концепцію відкритих даних і координує діяльність ентузіастів, IT-компаній та державних органів в Україні через соціально значимі IT-проекти, пов'язані з електронним урядом, електронної демократією, електронними послугами та відкритими урядовими даними. У 2014 році був розроблений законопроект про відкриті дані, прийнятий в першому читанні. Кабінет Міністрів розробив відповідну постанову про відкриття більш ніж 300 реєстрів і баз даних. У грудні 2017 року Кабінет міністрів України розширив перелік баз даних, які повинні публічно відкриватися державними органами, і кількість відкритих реєстрів зросла з 302 до 600. З 2013 по 2018 рік Україна поліпшила свою позицію в рейтингу Global Open Data Index. Наша країна стала однією з 50 найбільш відкритих держав, зайнявши 31-е місце. Точний розмір економічного потенціалу Open Data в даний час вивчається Київською школою економіки [6].

Серед ключових недоліків використання відкритих даних в Україні варто відзначити їхню неповноту, адже далеко не всі відомості, які мали б бути у відкритому доступі, представлені у відповідних реєстрах, а наявна інформація іноді подається лише частково. Проблемою є також некоректність відображення даних, коли в одному записі може міститися інформація про різних осіб або ж зазначаються помилкові ідентифікаційні коди юридичних осіб. Додаткові труднощі створює зміна стандартів даних, унаслідок чого змінюється структура чи формат публікацій, що призводить до збоїв у роботі автоматизованих сервісів і тимчасово обмежує користувачів у доступі до необхідної інформації. Важливою проблемою залишається і неактуальність даних, які не завжди оновлюються вчасно, а отже можуть бути застарілими або неточними. До цього додаються й технічні виклики, зокрема масовані кібератаки під час війни (особливо DDoS-атаки), що негативно впливають на стабільність роботи державних реєстрів та ускладнюють своєчасне отримання інформації користувачами [7].

Говорячи про переваги відкритих даних слід зазначити, що вони приносять грошову вигоду урядам і компаніям, скорочують витрати і покращують процеси прийняття рішень, створюють можливості для бізнесу і аналітиків даних. Open data здатна підвищувати прозорість та ефективність державного сектора, удосконалювати ділову практику, боротися з корупцією і ухиленням від податків. Сьогодні українці вже можуть отримувати і

використовувати тисячі файлів, опублікованих на data.gov.ua. Але багато громадян досі не знають про можливості відкритих даних. Поступово в Україні з'являється все більше можливостей використання опен дата: держава публікує інформацію, яка раніше була закрита, і підтримує проекти, спрямовані на використання відкритих даних [6].

Таким чином, використання відкритих даних в Україні у поєднанні з методами OSINT є потужним інструментом для підвищення прозорості, боротьби з корупцією та зміцнення інформаційної безпеки. Незважаючи на наявні недоліки – неповноту, неточність, неактуальність і технічні проблеми реєстрів – OpenData поступово розвивається і демонструє значний економічний та суспільний потенціал. Важливо, щоб держава і надалі вдосконалювала механізми публікації даних, а суспільство активніше використовувало їх у дослідженнях, бізнесі та сфері безпеки, адже саме у цьому полягає ключ до сталого розвитку й ефективної протидії сучасним викликам.

Список використаних джерел

1. Дія.Відкриті дані. URL: https://diia.data.gov.ua/info-center/wodi (дата звернення: 21.09.2025).
2. Що таке відкриті дані? – data.in.ua. data.in.ua. URL: https://www.data.in.ua/open-data/ (дата звернення: 21.09.2025).
3. OSINT - розвідка відкритих джерел: що це і чому варто замовити саме в Darkguard - DarkGuard. DarkGuard. URL: https://darkguard.com.ua/osint-rozvidka-vidkritih-dzherel-v-darkguard/ (дата звернення: 21.09.2025).
4. Maxym Z. Розвідка з відкритих джерел (Open-source intelligence - OSINT). Maxym Zosym. URL: https://www.maxzosim.com/rozvidka-z-vidkritikh-dzherel-osint/ (дата звернення: 21.09.2025).
5. vkarpova7. Як працює osint-розвідка? Від бізнес-аналізу до оборони україни. ISSP Training. URL: https://www.issp.training/post/yak-pratsyuye-osint-rozvidka-vid-biznes-analizu-do-oborony-ukrayiny (дата звернення: 21.09.2025).
6. Open data в Україні. YouControl як частина open data ua. YouControl. URL: https://youcontrol.com.ua/topics/open-data-otkryityie-dannyie-youcontrol/ (дата звернення: 21.09.2025).
7. Недоліки держреєстрів в Україні, які ускладнюють роботу з даними. YouControl. URL: https://youcontrol.com.ua/articles/nedoliky-derzhreiestriv-v-ukrayini,yaki-uskladniuiut-robotu-z-danymy/ (дата звернення: 21.09.2025).

Ключові слова: інформація, OSINT, розвідка, відкриті дані, вільний доступ, data.gov.ua, національна безпека, державні реєстри, закон «Про доступ до публічної інформації», переваги відкритих даних, інформаційна безпека.
Keywords: information, OSINT, intelligence, open data, free access, data.gov.ua, national security, state registers, law "On Access to Public Information", advantages of open data, information security.

ЗМІСТ