КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.749
УДК 004.056.5

Івкова Валерія Сергіївна
аспірант кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-2370-1497
valeriia.s.ivkova@lpnu.ua

Опірський Іван Романович
д.т.н., професор, завідувач кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

OSINT-ТЕХНОЛОГІЇ ЯК ЗАГРОЗА КІБЕРБЕЗПЕЦІ ДЕРЖАВИ

Анотація. У статті досліджено OSINT-технології, як один із ключових викликів для національної безпеки України. З розвитком цифрового простору методи збору, аналізу та використання інформації з відкритих джерел набули широкого поширення, зокрема у сфері кібербезпеки. Автори акцентують увагу на тому, що, попри легітимність і загальнодоступність OSINT-технологій, вони можуть бути використані зловмисниками для збору персональних даних, виявлення вразливостей у критичній інфраструктурі та планування кібератак. Дослідження ґрунтується на аналізі відкритих державних реєстрів, соціальних мереж, супутникових знімків, картографічних сервісів та інших джерел, які містять потенційно чутливу інформацію. Визначено основні загрози, пов'язані з OSINT, серед яких: викрадення персональних даних, фішинг, аналіз корпоративної інформації, несанкціоноване втручання у державні інформаційні системи. Окрему увагу приділено аналізу реальних інцидентів витоку інформації через OSINT-технології, включаючи приклади з міжнародної та української практики. Автори дослідили правові та етичні аспекти використання OSINT-інструментів, зокрема колізію між необхідністю відкритості державних даних та загрозами кібербезпеки. У статті наведено аналіз законодавчих норм України, що регулюють доступ до інформації, а також розглянуто міжнародний досвід у сфері протидії OSINT-загрозам. Окремий розділ статті присвячено методам протидії загрозам, які виникають через використання OSINT-інструментів. Також досліджено методи контр-OSINT (Counter-OSINT), що передбачають мінімізацію цифрового сліду, дезінформацію, анонімізацію даних, контроль за витоками інформації та використання засобів протидії OSINT-аналізу зображень і відео. Окремо розглянуто роль державних структур у розробці та впровадженні нормативно-правових актів, спрямованих на посилення захисту інформації у відкритих джерелах.

Ключові слова: OSINT; кібербезпека; контр-OSINT; персональні дані; витік інформації; національна безпека.

ВСТУП

В умовах збройної агресії російської федерації проти України, питання протидії проявам гібридної війни в інформаційному просторі постає все гостріше.

Згідно звіту про діяльність Департаменту кіберполіції Національної поліції України у 2024 році, найбільш характерними загрозами у кіберпросторі залишаються: фішинг, протиправний контент, онлайн-шахрайство, викрадення баз даних, втручання в роботу вебсайтів (кібератаки) [1].

В свою чергу урядова команда реагування на комп'ютерні надзвичайні події «CERT-UA», яка діє при Державній службі спеціального зв'язку та захисту інформації України, в 2024 році опрацювала 4315 кіберінцидентів, що на 69,8% більше, ніж у

2023 році, коли кіберзлочинці атакували український кіберпростір 2541 раз. Найпоширенішими типами інцидентів, згідно інформації Державної служби спеціального зв'язку є розповсюдження шкідливого програмного забезпечення, фішинг, шкідливе підключення, компрометація облікового запису або системи. Метою зловмисників є викрадення чутливої інформації, а також знищення даних та інформаційних систем. [2].

Окремим видом протиправної діяльності в кіберпросторі можна вважати поширення дезінформації та матеріалів пропагандистського характеру.

На підготовчому етапі, для кожного з видів цих злочинів та інцидентів безпеки, можуть бути використані OSINT-технології для виявлення персональних даних, конфіденційної інформації, вразливостей або збору інформації про об'єкт кібератаки.

Таким чином, проблема захисту критично важливої інформації, яка може міститься в відкритих джерелах інформації є нагальною та потребує негайного вирішення.

Постановка проблеми. Відсутність систематичного підходу до захисту інформації у відкритих джерелах, публікація даних, що, як приклад, містять відбитки печаток, скан-копії підписів чи електронний цифровий підпис створюють підґрунтя для компрометації цих даних та їх подальшого використання у протиправній діяльності. В тому числі такі відомості можуть бути використані на підготовчому етапі вчинення кібератак.

Одночасно з цим, чинне законодавство зобов'язує суб'єктів владних повноважень оприлюднювати ці дані [3], отже виникає колізія між дотриманням принципів відкритості і прозорості та питанням кібербезпеки.

Виходячи з вищенаведеного, врегулювання методів захисту інформації у відкритих джерелах інформації сприятиме підвищенню рівня захищеності окремих суб'єктів владних повноважень та держави в цілому.

Аналіз останніх досліджень і публікацій. Захист критично важливої інформації є постійним пріоритетом державних установ та організацій, оскільки від її безпеки залежить стабільність функціонування інфраструктури, економіки та національної безпеки загалом.

У контексті сучасних гібридних загроз і посилення кібератак, державні органи впроваджують системи кіберзахисту, здійснюють моніторинг інформаційного простору та проводять аудит безпеки ключових об'єктів. Особлива увага приділяється захисту даних, що стосуються військових об'єктів, енергетичної системи, транспортної інфраструктури та державних реєстрів. Водночас важливою складовою є навчання персоналу та запровадження жорстких політик доступу до конфіденційної інформації, аби мінімізувати ризики витоку даних через людський фактор чи технічні вразливості.

Окремо слід враховувати, використання соціальних мереж працівниками державних підприємств, установ організацій з метою публікації як робочої інформації так і ведення особистих профілів.

Як приклад, Йонг-Джун Лі, Парк Се-Джун, Парк Вон-Хен в своєму дослідженні «Military Information Leak Response Technology through OSINT Information Analysis Using SNSes» зазначають, що в результаті проведення експерименту з використанням усього чотирьох OSINT-систем, за пошуковими запитами з дев'яти ключових слів, які пов'язані з військовою інформацією, а саме: «військова таємниця», «обороно-промислові переваги», «оборонні компанії», «оборонний потенціал», «проекти вдосконалення», «офіцери», «системи озброєння» та «оборонні проекти», введеними англійською мовою, отримали 100209 результатів використання ключових слів в соціальних мережах [4, с. 4].

В Україні подібні дослідження не проводились, проте відповідно до звітів основних суб'єктів забезпечення кібербезпеки — соціальні мережі на постійній основі

використовуються зловмисниками для збору інформації про об'єкт атаки, зокрема для поширення фішингових посилань, шкідливого програмного забезпечення, вчинення несанкціонованих втручань в роботу електронно-обчислювальної техніки, тощо.

Метою статті є дослідження і аналіз алгоритмів для захисту інформації у відкритих джерелах інформації та визначення проблематики і перспективних напрямів їх застосування в Україні, в контексті кібербезпеки держави від використання даних в OSINT-технологіях.

Завданнями дослідження є:

1. Дослідити OSINT-технології як інструмент потенційної загрози.
2. Виявити шляхи мінімізації ризиків для держави.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

OSINT-технології: суть і розвиток

OSINT — метод пошуку інформації з відкритих джерел. Відкритими джерелами прийнято вважати загальнодоступні відомості, які наприклад містяться в соціальних мережах, веб-сайтах, форумах або інших ресурсах, доступ до яких не обмежений володільцем або розпорядником таких даних.

В розрізі вивчення OSINT, як сукупної технології пошуку інформації у відкритих джерелах, дослідники поділяють його на декілька типів.

Наприклад, вчені з республіки Корея Йон-Вун Хван, Ім-Йонг Лі, Хванкук Кім, Хеджун Лі, Донгхюн Кім поділяють OSINT-технології за наступним принципом: OSINT (розвідка по відкритих джерелах), HUMINT (отримання інформації від людини, так звана «агентурна розвідка») та TECHINT (технології та інформаційні ресурси використовуються для збору розвідданих противника, включає в себе IMINT, SIGINT, MASINT) [5, с. 2].

Одночасно з цим, румунський вчений Андрей Сандор описує нові напрямки розвитку OSINT-технологій, як CYBERINT (Cyber Intelligence) та SOCMINT (Social Media Intelligence) [6, с. 151].

На нашу думку, поняття OSINT-технології необхідно сприймати, як комплекс методів та засобів для отримання інформації з відкритих джерел, які включають в себе підгрупи або напрямки досліджень в залежності від об'єкту або методології розвідки.

Таблиця 1

Різновиди розвідки та джерела інформації

Вид розвідки	Сутність методу	Джерела інформації
OSINT (Open source intelligence) * в класичному розумінні	збір даних з відкритих загальнодоступних джерел інформації, доступ до якої не обмежений розпорядником або власником інформації	Відкриті загальнодоступні джерела інформації в мережі Інтернет
HUMINT (Human intelligence)	збір відомостей від агентурних джерел або шляхом спілкування з людьми. В інформаційному середовищі такий вид розвідки може ототожнюватися з «соціальною інженерією».	Веб-сайти установ, організацій, підприємств, електронна пошта, соціальні мережі, тощо
IMINT (Imagery Intelligence)	розвідка по зображеннях об'єктів (місцевість, забудова, особа, тощо), які відтворюються за допомогою електронних або оптичних засобів.	Соціальні мережі, форуми, сервіси обміну зображеннями, агрегати зображень.

SIGINT (Signals intelligence)	розвідка, використання якої передбачає перехоплення сигналів, як між людьми так і між машинами, або комбіновано.	Радіосигнали, wifi, тощо
MASINT (Measurement and signature intelligence)	збір інформації, що передбачає пошук і аналіз даних, отриманих із специфічних технічних та наукових джерел	Наукометричні бази
GEOINT (Geospatial Intelligence)	розвідка по геопросторових даних	Мапи, агрегатори онлайн зображень, метадані
TECHINT (Technical intelligence)	розвідка про озброєння та техніку, що використовуються збройними силами іноземних держав	Соціальні мережі, сайти установ та організацій
CYBERINT (Cyber Intelligence)	це підобласть кібербезпеки, яка фокусується на структурованому зборі, аналізі та поширенні даних про потенційні або існуючі кіберзагрози	Агрегатори для пошуку вразливостей, сканери, відкриті порти, ін.
SOCMINT (Social Media Intelligence)	збір розвідувальної інформації з соціальних медіа, використовуючи нав'язливі та ненав'язливі засоби від відкритих та закритих соціальних мереж	Соціальні мережі та месенджери
FININT (Financial intelligence)	це збір інформації про фінансові справи суб'єктів, з метою розуміння їх характеру і можливостей та подальшого передбачення їх наміри	Податкові звіти, реєстр декларацій
MARKINT (Market intelligence)	збір та аналіз інформації, що стосуються ринку компанії — тенденції, моніторинг конкурентів і клієнтів (існуючих, втрачених і цільових)	Сайти підприємств, установ, організацій; бази тендерних закупівель, профілі співробітників у соціальних мережах

Наразі, OSINT-технології розглядаються як інформаційно-аналітичний підхід, що передбачає збір, обробку та аналіз даних із відкритих джерел, таких як медіа, соціальні мережі, онлайн-бази даних, наукові публікації та інші публічно доступні джерела. Завдяки своїй універсальності цей метод знайшов широке застосування як у державному, так і приватному секторах, а також у середовищі кіберзлочинців.

Зокрема в державному секторі OSINT, може використовуватися забезпечення національної безпеки, проведення стратегічної розвідки, протидії злочинності та забезпечення кібербезпеки, в свою чергу приватний сектор використовує OSINT для конкурентної розвідки, репутаційного моніторингу, виявлення ризиків (оцінка надійності партнерів), забезпечення кіберзахисту.

Попри значний позитивний потенціал OSINT, цей інструмент активно використовується кіберзлочинцями для підготовки до вчинення протиправної діяльності.

Соціальна інженерія та фішинг: аналіз відкритих джерел дозволяє зловмисникам збирати персональні дані потенційних жертв для створення персоналізованих атак, які значно підвищують їхню ефективність.

Виявлення вразливостей: кіберзлочинці аналізують інформацію з технічних форумів, блогів розробників та інших відкритих джерел для пошуку вразливостей у програмному забезпеченні або IT-інфраструктурі.

Аналіз корпоративних даних: зловмисники збирають публічні дані про компанії, такі як структура бізнесу, ключові співробітники та їхня діяльність, що може бути використано для організації атак.

Несанкціонований збут інформації: кіберзлочинці використовують OSINT для пошуку витоків даних, які згодом можуть бути продані на нелегальних платформах.

ISSN 2663 - 4023

Таким чином, OSINT є потужним інструментом, який забезпечує державні та приватні організації критично важливою інформацією для прийняття рішень, але водночас створює серйозні виклики у сфері кіберзахисту та безпеки.

OSINT як загроза для державної безпеки

Однією з ключових загроз, що виникає через відкриті джерела інформації, є можливість збору та аналізу даних про об'єкти критичної інфраструктури, зокрема транспортну систему, енергетичні мережі, стратегічні підприємства.

Основними джерелами такої інформації є:

- **Геолокаційні сервіси**: платформи на кшталт Google Maps, OpenStreetMap та інших картографічних сервісів дозволяють отримувати точні координати стратегічно важливих об'єктів, зокрема військових баз, заводів оборонного комплексу, електростанцій чи транспортних вузлів.

Наприклад, у 2018 році стався інцидент, коли фітнес-додаток «Strava» опублікував глобальну «теплову» карту, яка випадково розкрила місцезнаходження секретних військових баз, включаючи об'єкти в Україні. Це стало можливим через те, що користувачі, зокрема військовослужбовці, ділилися маршрутами своїх тренувань в соціальних мережах, що призвело до витоку чутливих геолокаційних даних [7].

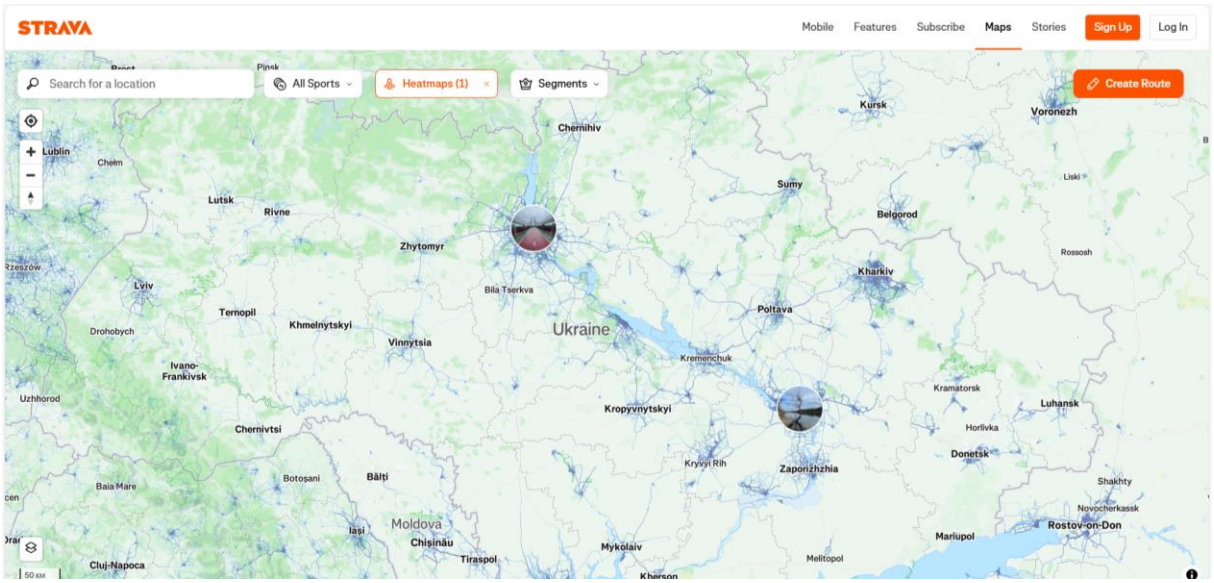

Рис. 1. Приклад теплової карти додатку «Strava»

- **Відкриті державні реєстри**: публічні кадастрові карти, реєстри юридичних осіб та інші офіційні бази даних можуть надавати інформацію про власників об'єктів критичної інфраструктури, їхні функції та потужності.

В Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань міститься контактна інформація підприємств, зокрема адреси реєстрації, які часто співпадають з місцем фактичного здійснення діяльності, інформація про власників та керівників, а також номери телефонів або адреси електронних поштових скриньок. В сукупності вказана інформація надає можливість створити профіль підприємства та сформувати вектор атаки.

ISSN 2663 - 4023

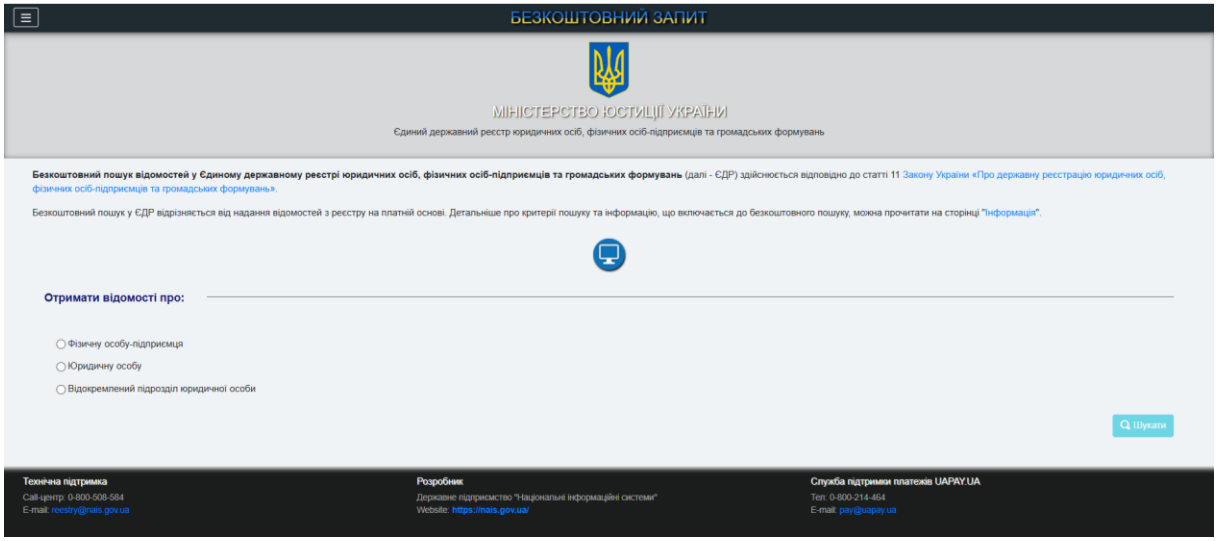

Рис. 2. Форма онлайн-запиту на отримання інформації з ЄДР

- **Супутникові зображення**: безкоштовні та комерційні супутникові платформи, такі як Sentinel Hub або Maxar Technologies, дозволяють відслідковувати зміни на об’єктах у режимі реального часу, що створює ризики для національної безпеки.

Як приклад, в листопаді 2024 року, після оновлення на картах «Google» з’явились супутникові знімки з розташуванням військових систем України. В результаті інциденту, в прес-службі корпорації повідомили, що знімки зроблені понад рік тому із загальнодоступних джерел. Враховуючи військову агресії рф проти України, публікація такого роду інформації становить загрозу національній безпеці [8].

Рис. 3. Ілюстративне зображення. Скріншот карти Google Maps

- **Сервіси збору даних про IT-інфраструктуру та вразливості**: безкоштовні та комерційні платформи з дослідження IT-інфраструктури та вразливостей системи, зокрема shodan.io, censys.com та інші, надають інформацію про вразливості та запущені служби на вузлі, що надає можливість подальшої експлуатації загрози або підбору методів та засобів для вчинення атаки.

ISSN 2663 - 4023

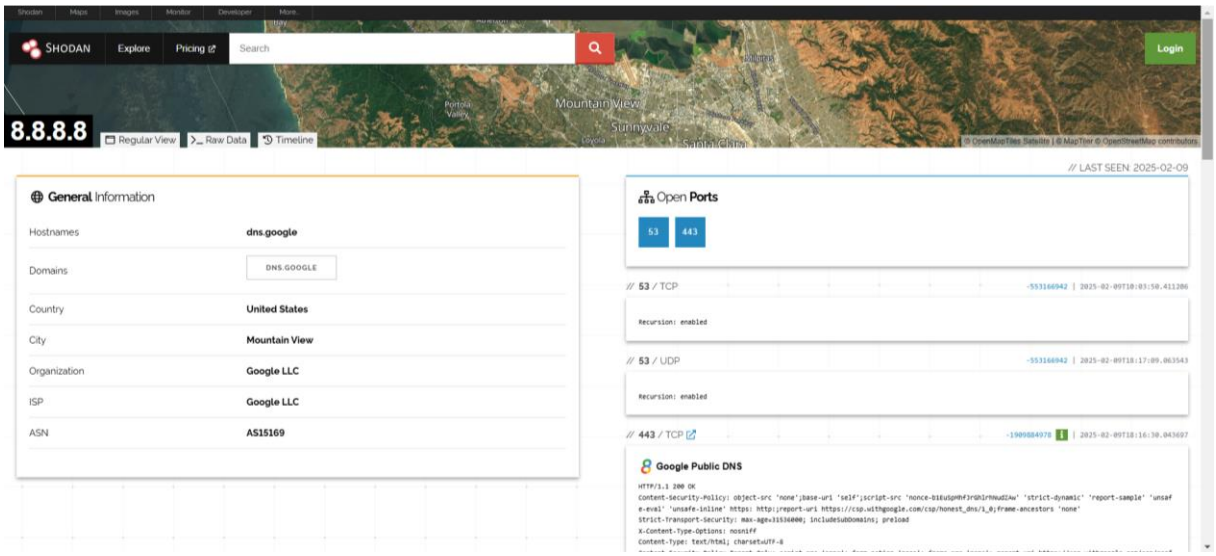

Рис. 4. Приклад виводу інформації сервісом Shodan

Юридичні та етичні аспекти обмеження OSINT

Згідно ч.1 ст. 5 Закону України «Про доступ до публічної інформації» відомості, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених Законом, та інформація, що становить суспільний інтерес має бути доступна та підлягає систематичному та оперативному оприлюдненню в офіційних друкованих виданнях; на офіційних веб-сайтах в мережі Інтернет та на єдиному державному веб-порталі відкритих даних. Обмеження щодо поширення вищевказаних даних накладається лише конфіденційну, службову та таємну інформацію [3].

Офіційні друковані видання, офіційних веб-сайти в мережі Інтернет та єдиний державний веб-портал відкритих даних — є публічно доступними сервісами, а отже можуть бути джерелом інформації для використання OSINT-технологій.

Відповідно до Закону України «Про доступ до публічної інформації» та внутрішніх розпорядчих документів державні установи, підприємства та організації оприлюднюють, в тому числі розпорядчі документи, які як приклад, містять відбитки печаток, скан-копії підписів чи електронний цифровий підпис, чим створюють підґрунтя для компрометації цих даних та їх подальшого використання у протиправній діяльності.

Станом на лютий 2025 року, жодної іншої форми верифікації документу законодавчо не впроваджено. Відповідно перевірити легітимність документу можливо або через офіційні повідомлення (підтвердження або спростування) установ або їх представників, або в порядку, передбаченому Законом України «Про звернення громадян».

Так, в лютому 2025 року, Центр протидії дезінформації повідомив про поширення підробленого документу, нібито виданого Головним управлінням Національної поліції в Одеській області, у якому йдеться про начебто наказ правоохоронцям «посилити пошук осіб, які підлягають мобілізації».

«Документ» містить стилістичні помилки та невідповідність формату офіційних розпоряджень. Також, за даними Центру протидії дезінформації, під вказаним у «документі» номером насправді зареєстрований зовсім інший наказ — про звільнення колишньої працівниці ГУНП в Одеській області, датований 31.10.2024. [9].

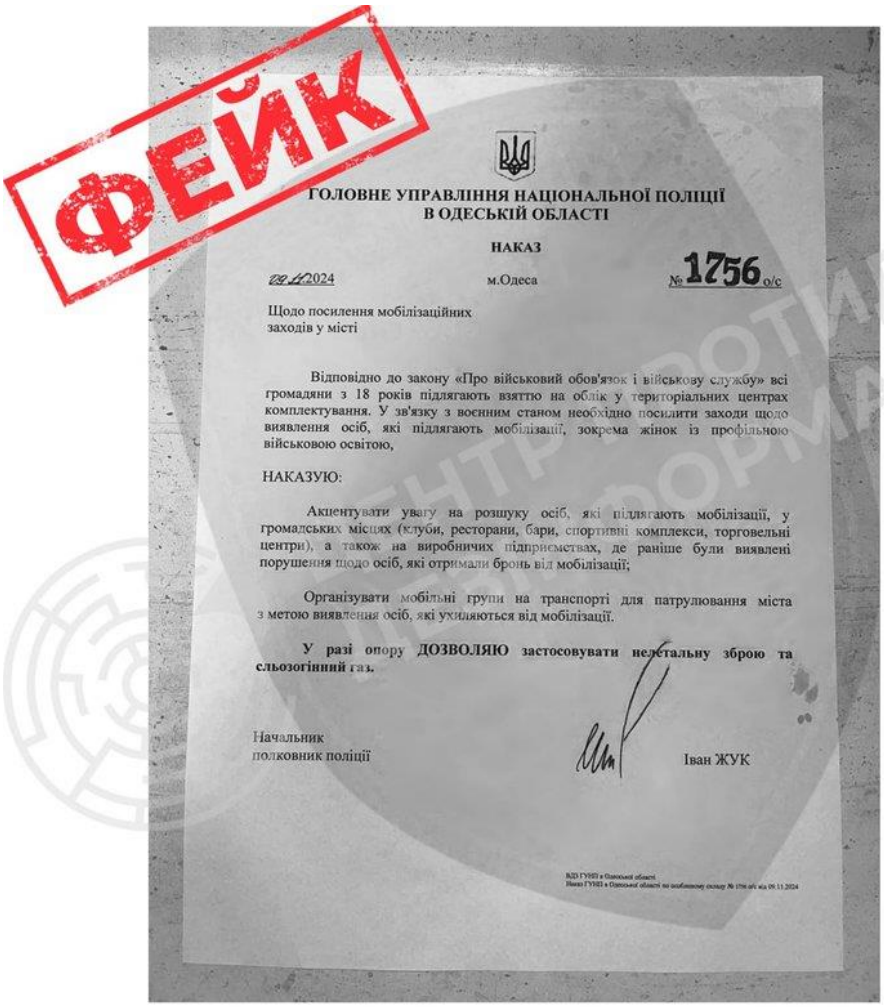

Рис. 5. Приклад підробки документів від державних установ

Окремого врегулювання потребують питання ведення публічних профілів в соціальних мережах від імені державних установ, підприємств та організацій, та як уніфікованого нормативно-правового акту щодо правил публікації відомостей не існує.

Крім цього, більша частка витоків інформації припадає на особисті профілі співробітників в соціальних мережах та месенджерах, так не поодинокими є випадки публікації зображення документів чи їх частин, внутрішньої інфраструктури приміщень, обладнання та іншої інформації.

Одночасно з цим, гостро стоїть питання дотримання політики безпеки, як приклад, через недотримання вимог передачі відомостей, працівники установи можуть поширювати документи через месенджери. У зв’язку з цим, у випадку компрометації акаунту через фішингове посилання, вся інформація буде доступна зловмиснику.

На даний час, відомості про логіни, паролі, контактна інформація (сторінки в соціальних мережах, нікнейми в месенджерах, номери мобільних телефонів або адреси сервісів електронної пошти), фотографії, тощо, розміщені у відкритому доступі, не підпадають під визначення «конфіденційної інформації» або «персональних даних», зафіксовані в національному законодавстві, а їх використання в Україні регламентоване лише політиками конфіденційності окремих електронних ресурсів, які кожен утримувач такого ресурсу визначає самостійно [10, с. 191].

Використання загальнодоступних даних в Україні регламентовано Законом України «Про доступ до публічної інформації», однак збір відомостей про певну особу, з метою подальшого використання, в тому числі конфіденційних даних, без згоди особи, може тягнути за собою кримінальну відповідальність, за ст. 182 (Порушення недоторканності приватного життя) КК України, а відповідальність за незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю передбачена ст. 231 КК України [11].

Етична сторона використання OSINT-технологій полягає у порушенні права на конфіденційність, оскільки вони можуть включати збір інформації про приватних осіб або організації без їх відома або згоди.

Технологічні засоби захисту інформації

Захист критично важливої інформації в умовах сучасних кіберзагроз вимагає впровадження передових технологічних рішень. Одними з ключових механізмів є системи шифрування, платформи моніторингу інформаційного простору та засоби запобігання витоку конфіденційних даних.

- **Шифрування даних** — дозволяє захистити інформацію як під час передачі, так і при її зберіганні. Використання асиметричних і симетричних алгоритмів шифрування (AES, RSA) забезпечує високий рівень конфіденційності.
- **VPN та захищені канали зв'язку** — забезпечують приватність у комунікаціях шляхом приховування реальної IP-адреси та створення захищеного тунелю між користувачами.
- **Електронні цифрові підписи** — забезпечують автентичність і цілісність переданих документів чи повідомлень**.**
- **Інструменти для анонімізації:** Tor, I2P та інші платформи сприяють захисту особистих даних та анонімності в мережі.

Платформи для моніторингу та мінімізації витоку інформації

- **DLP-системи (Data Loss Prevention):** автоматично відстежують і блокують передачу конфіденційної інформації поза корпоративну мережу, забезпечуючи контроль над даними.
- **SIEM-платформи (Security Information and Event Management):** дозволяють збирати, аналізувати та корелювати події безпеки, а також виявляти потенційні загрози.
- **Системи моніторингу відкритих джерел (OSINT):** аналізують інформаційний простір для виявлення витоків даних про критичну інфраструктуру чи конфіденційну інформацію.
- **Антивірусне та антишпигунське програмне забезпечення:** забезпечують базовий рівень захисту від шкідливого програмного забезпечення, яке може бути використане для збору даних.
- **Брандмауери та системи IDS/IPS:** дозволяють захищати мережі від несанкціонованого доступу та кіберзагроз.

Використання комплексного підходу, що включає шифрування, моніторинг загроз та активне управління ризиками, є запорукою ефективного захисту критичної інформації.

Освітні заходи для підвищення обізнаності у сфері кібербезпеки в контексті захисту держави від OSINT-технологій. У сучасному цифровому середовищі розвідка на основі відкритих джерел (OSINT) стала потужним інструментом збору інформації, який використовується як державними структурами, так і зловмисниками. Зростання ролі OSINT у розвідувальній діяльності обумовлює необхідність підвищення обізнаності громадян та фахівців щодо методів захисту від можливих загроз, пов'язаних із використанням відкритих даних.

В Україні реалізується низка освітніх програм, спрямованих на підвищення рівня кібергігієни та обізнаності про онлайн-загрози. Зокрема, проєкт «Дія.Освіта» спільно з USAID «Кібербезпека критично важливої інфраструктури України» запустили інформаційну кампанію, метою якої є навчання українців основам кібергігієни та захисту в цифровому просторі [12].

Крім того, платформа Prometheus пропонує курс «OSINT — розвідка з відкритих джерел та інформаційна безпека», який допомагає опанувати інструменти OSINT, навчитися розпізнавати дезінформацію та захищати приватні дані.

Таким чином, з метою протидії можливим загрозам, пов'язаним із використанням OSINT-технологій, важливо впроваджувати освітні заходи, які охоплюють:

1. **Розвиток навичок кібергігієни**: навчання безпечному використанню інтернету, управлінню конфіденційною інформацією та розпізнаванню фішингових атак.
2. **Опанування інструментів OSINT**: розуміння принципів роботи з відкритими джерелами, що дозволяє виявляти потенційні загрози та запобігати витоку інформації.
3. **Підвищення обізнаності про інформаційну безпеку**: проведення тренінгів та семінарів для державних службовців та громадян щодо захисту від інформаційних атак та маніпуляцій.

Таким чином, впровадження комплексних освітніх заходів є ключовим елементом у зміцненні кібербезпеки держави та захисті від потенційних загроз, пов'язаних із використанням OSINT-технологій.

Окремо слід зауважити на необхідності впровадження **контр-OSINT методів.**

Контр-OSINT (Counter-OSINT) — це набір методів і стратегій, спрямованих на захист інформації від збору, аналізу та використання зловмисниками через відкриті джерела. Основні контрзаходи включають обмеження доступу до чутливих даних, дезінформацію та контроль за цифровим слідом.

1. Мінімізація цифрового сліду

Цифровий слід — це інформація, яку користувач залишає в мережі (профілі в соціальних мережах, геопросторові дані, тощо). Його скорочення допомагає зменшити ризик збору OSINT-даних.

- **Обмеження особистої інформації**: видалення або приховування даних у соціальних мережах, обмеження доступу до фотографій, геолокації, професійних контактів.
- **Використання анонімних акаунтів** для роботи в інтернеті (наприклад, VPN, TOR, анонімні електронні адреси).
- **Відмова від безкоштовних сервісів**, які збирають і аналізують персональні дані (наприклад, Google, Facebook, LinkedIn).

2. Дезінформація та введення в оману

Один із ефективних методів захисту — навмисне поширення хибних або неповних даних, щоб ускладнити аналіз для OSINT-дослідників.

- **Створення фальшивих профілів**: наповнення їх некоректною інформацією, яка відволікатиме аналітиків.
- **Маніпуляція даними**: зміна дат, геолокації, подій, використання фальшивих цифрових слідів.
- **Підміна технічної інформації**: маскування реального IP-адреси, використання шифрованих комунікацій (Signal, ProtonMail).

3. Контроль за витоками інформації

Витоки конфіденційних даних можуть траплятися через зламані акаунти, несанкціонований доступ або витік від третіх осіб.

- **Використання багаторазової автентифікації (2FA)** для захисту облікових записів.
- **Регулярний аудит безпеки**: перевірка витоків паролів, доступності інформації про користувача в пошукових системах (Google Dorking).
- **Використання спеціальних сервісів (Have I Been Pwned, Dehashed)** для перевірки, чи потрапили особисті дані у відкритий доступ.

4. Захист від OSINT-аналізу зображень і відео

Фотографії та відео містять метадані, які можуть бути використані для аналізу місцезнаходження та інших параметрів.

- **Видалення EXIF-метаданих** перед публікацією фото (за допомогою Metastripper, ExifCleaner).
- **Уникнення публікації геолокації** або розмиття важливих деталей на зображеннях.
- **Затримка в часі при публікаціях** для унеможливлення визначення поточного місцезнаходження.

5. Захист корпоративної та державної інформації

OSINT часто використовується для збору інформації про компанії та урядові структури.

- **Обмеження відкритого доступу до документів** (PDF, DOCX), які можуть містити метадані про організацію.
- **Моніторинг згадок у мережі** (Google Alerts, Meltwater, Mention) для виявлення витоків інформації.
- **Проведення тренінгів з кібергігієни** для співробітників, щоб мінімізувати ризик ненавмисного розкриття інформації.

Контр-OSINT методи є важливим компонентом сучасної інформаційної безпеки. Вони допомагають зменшити ризик збору критичних даних, ускладнити діяльність розвідників і мінімізувати загрози, пов’язані з відкритими джерелами. Ефективна стратегія передбачає поєднання технічних заходів, інформаційного контролю та навчання користувачів безпечній поведінці в цифровому середовищі.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Дослідження OSINT-технологій як інструменту потенційної загрози дозволило встановити, що розвідка на основі відкритих джерел відіграє значну роль у сучасному інформаційному просторі. Використання OSINT може призвести до витоку

конфіденційної інформації, сприяти проведенню кібератак, маніпуляціям громадською думкою та іншим формам інформаційного впливу. Особливо це актуально в контексті державної безпеки, де зловмисники можуть застосовувати відкриті дані для ідентифікації критично важливої інфраструктури, посадових осіб та стратегічних об'єктів.

З метою мінімізації ризиків, пов'язаних із OSINT, визначено такі ключові напрями:

1. **Освітні заходи та підвищення цифрової грамотності** — впровадження навчальних програм з кібергігієни та інформаційної безпеки для державних службовців, військових, представників критичної інфраструктури та широкого загалу громадян.
2. **Регулювання доступу до відкритих даних** — удосконалення політики розкриття державної інформації, обмеження публікації потенційно небезпечних даних, зокрема геолокації, персональних відомостей та технічних характеристик стратегічних об'єктів.
3. **Використання контр-OSINT методів** — впровадження технологій для відстеження витоку інформації, анонімізації даних та протидії ворожим OSINT-операціям.
4. **Розвиток міжвідомчої співпраці** — координація зусиль державних органів, бізнесу та громадянського суспільства у сфері кібербезпеки для оперативного реагування на загрози та вдосконалення механізмів протидії.

Таким чином, підвищення обізнаності про OSINT-загрози та розбудова національної стратегії захисту відкритих даних є необхідними складовими державної кібербезпеки. Впровадження комплексного підходу дозволить знизити ризики, пов'язані із використанням OSINT-технологій, та підвищити стійкість країни до інформаційних загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Report on the activities of the CyberPolice Department of the National Police of Ukraine in 2024 (2025).* CyberPolice Department of the National Police of Ukraine. https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/
2. *CERT-UA processed 4315 cyber incidents last year.* (2025) State Service for Special Communications and Information Protection of Ukraine. https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv
3. On Access to Public Information, Law of Ukraine № 2939-VI (2023) (Ukraine). https://zakon.rada.gov.ua/laws/show/2939-17#Text
4. Lee, Y.-J., Park, S.-J., & Park, W.-H. (2022). Military Information Leak Response Technology through OSINT Information Analysis Using SNSes. *Security and Communication Networks,* 2022, 1–10. https://doi.org/10.1155/2022/9962029
5. Hwang, Y.-W., Lee, I.-Y., Kim, H., Lee, H., & Kim, D. (2022). Current Status and Security Trend of OSINT. *Wireless Communications and Mobile Computing*, 2022, 1–14. https://doi.org/10.1155/2022/1290129
6. Şandor, A. (2020). An Intelligence Perspective on Privacy and Data Protection Risks in Social Media. *International conference KNOWLEDGE-BASED ORGANIZATION, 26(1),* 151–156. https://doi.org/10.2478/kbo-2020-0023
7. Hsu, J. (2018). *The Strava Heat Map Shows Even Militaries Can't Keep Secrets from Social Data.* WIRED. https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/
8. Lutovych, D. (2024). *Google "leaked" data on the location of Ukrainian troops: what is the danger.* FOCUS. https://focus.ua/uk/voennye-novosti/676818-google-onoviv-karti-i-viyaviv-roztashuvannya-ukrajinskiy-viyskovih-ob-yektiv

9. *Fake order to strengthen mobilization measures in Odessa* (2024) Center for Countering Disinformation. https://cpd.gov.ua/international-direction/ssha/fejkovyj-nakaz-pro-posylennya-mobilizaczijnyh-zahodiv-v-odesi/
10. Ivkova, V., & Opirsky, I. (2024). RESEARCH ON THE ISSUES OF PROVIDING SECURITY OF PERSONAL DATA AND CONFIDENTIAL INFORMATION IN THE CONTEXT OF OSINT COUNTERACTION. *Electronic professional scientific publication "Cybersecurity: education, science, technology"*, 2(26), 189–199. https://doi.org/10.28925/2663-4023.2024.26.682
11. Criminal Code of Ukraine, Law of Ukraine № 2341-III (2025) (Ukraine) https://zakon.rada.gov.ua/laws/show/2341-14#Text
12. *Diya.Osvita and USAID Cybersecurity Project launch cyber hygiene information campaign.* (n.d.). Ministry of Digital Transformation of Ukraine. https://thedigital.gov.ua/news/diyaosvita-ta-proekt-usaid-kiberbezpeka-zapuskayut-informatsiynu-kampaniyu-z-kibergigieni

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Valeriia Ivkova
Postgraduate Student of Information Protection Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-2370-1497
valeriia.s.ivkova@lpnu.ua

Ivan Opirskyy
Doctor of Science, Professor, Head of Information Protection Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

OSINT TECHNOLOGIES AS A THREAT TO STATE CYBERSECURITY

Abstract. The article examines OSINT technologies as one of the key challenges for the national security of Ukraine. With the development of the digital space, methods of collecting, analyzing and using information from open sources have become widespread, in particular in the field of cybersecurity. The authors emphasize that, despite the legitimacy and general availability of OSINT technologies, they can be used by attackers to collect personal data, identify vulnerabilities in critical infrastructure and plan cyberattacks. The study is based on the analysis of open state registers, social networks, satellite images, mapping services and other sources containing potentially sensitive information. The main threats associated with OSINT are identified, including: theft of personal data, phishing, analysis of corporate information, unauthorized interference in state information systems. Special attention is paid to the analysis of real incidents of information leakage through OSINT technologies, including examples from international and Ukrainian practice. The authors have examined the legal and ethical aspects of the use of OSINT tools, in particular the conflict between the need for openness of state data and cybersecurity threats. The article provides an analysis of the legislative norms of Ukraine that regulate access to information, and also considers international experience in the field of countering OSINT threats. A separate section of the article is devoted to methods of countering threats that arise through the use of OSINT tools. Counter-OSINT methods are also studied, which involve minimizing the digital trace, disinformation, data anonymization, control over information leaks, and the use of means of countering OSINT analysis of images and videos. The role of state structures in the development and implementation of regulatory legal acts aimed at strengthening the protection of information in open sources is separately considered.

Keywords: OSINT; cybersecurity; counter-OSINT; personal data; information leak; national security.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. *Report on the activities of the CyberPolice Department of the National Police of Ukraine in 2024 (2025).* CyberPolice Department of the National Police of Ukraine. https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/
2. *CERT-UA processed 4315 cyber incidents last year.* (2025) State Service for Special Communications and Information Protection of Ukraine. https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv
3. On Access to Public Information, Law of Ukraine № 2939-VI (2023) (Ukraine). https://zakon.rada.gov.ua/laws/show/2939-17#Text
4. Lee, Y.-J., Park, S.-J., & Park, W.-H. (2022). Military Information Leak Response Technology through OSINT Information Analysis Using SNSes. *Security and Communication Networks*, 2022, 1–10. https://doi.org/10.1155/2022/9962029
5. Hwang, Y.-W., Lee, I.-Y., Kim, H., Lee, H., & Kim, D. (2022). Current Status and Security Trend of OSINT. *Wireless Communications and Mobile Computing*, 2022, 1–14. https://doi.org/10.1155/2022/1290129

6. Șandor, A. (2020). An Intelligence Perspective on Privacy and Data Protection Risks in Social Media. *International conference KNOWLEDGE-BASED ORGANIZATION*, *26(1)*, 151–156. https://doi.org/10.2478/kbo-2020-0023
7. Hsu, J. (2018). *The Strava Heat Map Shows Even Militaries Can't Keep Secrets from Social Data.* WIRED. https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/
8. Lutovych, D. (2024). *Google "leaked" data on the location of Ukrainian troops: what is the danger.* FOCUS. https://focus.ua/uk/voennye-novosti/676818-google-onoviv-karti-i-viyaviv-roztashuvannya-ukrajinskiy-viyskovih-ob-yektiv
9. *Fake order to strengthen mobilization measures in Odessa* (2024) Center for Countering Disinformation. https://cpd.gov.ua/international-direction/ssha/fejkovyj-nakaz-pro-posylennya-mobilizaczijnyh-zahodiv-v-odesi/
10. Ivkova, V., & Opirsky, I. (2024). RESEARCH ON THE ISSUES OF PROVIDING SECURITY OF PERSONAL DATA AND CONFIDENTIAL INFORMATION IN THE CONTEXT OF OSINT COUNTERACTION. *Electronic professional scientific publication "Cybersecurity: education, science, technology"*, 2(26), 189–199. https://doi.org/10.28925/2663-4023.2024.26.682
11. Criminal Code of Ukraine, Law of Ukraine № 2341-III (2025) (Ukraine) https://zakon.rada.gov.ua/laws/show/2341-14#Text
12. *Diya.Osvita and USAID Cybersecurity Project launch cyber hygiene information campaign.* (n.d.). Ministry of Digital Transformation of Ukraine. https://thedigital.gov.ua/news/diyaosvita-ta-proekt-usaid-kiberbezpeka-zapuskayut-informatsiynu-kampaniyu-z-kibergigieni