РОЗВІДКА ВІДКРИТИХ ДЖЕРЕЛ (OPEN SOURCE INTELLIGENCE)

Ржевська Н.Ф., Кожушко О.О.*

кандидат політичних наук,
**магістрант спеціальності «міжнародна інформація»*
Інститут міжнародних відносин Національного авіаційного університету

Для прийняття зваженого та ефективного рішення необхідно володіти інформацією, що сприяла б процесу вироблення такого рішення, а отже – була б повною, актуальною, точною і релевантною. Сьогодні існують різноманітні методи збору інформації, що використовуються комплексно або окремо. Одним з таких є розвідка відкритих джерел.

Поділ розвідки на відкриту і таємну насправді виглядає досить умовно. Значна частина агентурної розвідки проводиться відкритим шляхом через обізнаних людей, наприклад, розпитування біженців, бесіди з туристами, звіти послів, аташе, торгових представників.

Важливим напрямом удосконалення роботи розвідувальних органів є створення ефективної системи отримання інформації з відкритих джерел (подібні системи створені у розвідках провідних країнах світу). Водночас в умовах відкритого інформаційного простору та вільного доступу до інформації організація такої роботи є надзвичайно складною і потребує значних фінансових видатків, застосування новітніх технологій та підходів. Разом з тим, як свідчить досвід розвідок провідних країн світу, ефективна робота такої системи є для вищих посадових осіб держави видимою якісною характеристикою щоденної роботи розвідувальних служб і певною мірою показовим чинником їх затребуваності. З іншого боку, системна робота з відкритими джерелами інформації суттєво доповнює інформаційні можливості самих розвідувальних органів [1].

OSINT(Open source intelligence) – розвідка відкритих джерел – це завжди специфічна інформація, зібрана й структурована особливим чином для відповіді на конкретні запитання [2].

Формування даного поняття відбувалося шляхом трансформації поняття «інформація з відкритих джерел» (open source information (OSIF). У спрощеному варіанті, даний термін стосується інформації, що не має грифу «таємно». Розвідувальне співтовариство США (Intelligence Community) визначає таку інформацію як загальнодоступний матеріал,

що може отримати кожен законним шляхом через запит, купівлю чи спостереження. Збір такої інформації повинен відповідати діючим вимогам захисту авторських прав [4].

Відкриті джерела інформації можна розділити на 4 категорії [4]:

1. широко розповсюджені дані та інформація;
2. цільові комерційні дані;
3. експертні оцінки;
4. «сіра» література.

Довідник НАТО (NATO Open Source Intelligence Reader) акцентує увагу на категорії «сіра література». Вона може включати наукові доповіді, технічні інструкції, економічні звіти, робочу документацію, неофіційні урядові документи, дисертації, маркетингові дослідження, інформаційні бюлетені та багато іншого. Всі ці матеріали охоплюють наукову, політичну, соціально-економічну та військову сфери [5].

З точки зору термінології, що використовується у розвідці, OSINT є релевантною щодо вимог розвідки інформацією, отриманою шляхом систематичного збору, обробки та аналізу публічно відкритої інформації. Цей термін включає два взаємодоповнюючих компонента [6]:

- відкрите джерело – інформація, що надана особою чи групою без сподівань на конфіденційність;
- доступна для громадськості інформація – дані, факти, інструкції, або інші матеріали, опубліковані чи передані широкому загалу, доступні на вимогу будь-якої людини, законно побачені або почуті будь-яким випадковим спостерігачем, чи розголошені на зустрічах відкритих широкій публіці.

У довіднику НАТО (NATO Open Source Intelligence Handbook) також використовується поняття Open Source Data (OSD), дані – неопрацьована друкована, ефірна, усна або інша форма інформації з першоджерел. Це можуть бути фотографії, аудіо записи, супутникові зображення, приватна переписка [7].

Відкриті джерела та публічно доступні відомості можуть включати в себе, але не обмежені наступними видами [6]:

– *академічна сфера* – програмне забезпечення, дисертації, лекції, презентації, дослідницькі роботи, знання в друкованому та електронному вигляді з економіки, географії (фізична, культурна, військово-політична), міжнародних відносин, регіональної безпеки, науки і технологій;

– *державні, міждержавні та недержавні організації (NGOs)* – бази даних, оприлюднена інформація, і друковані звіти, огляди широкого спектру в економіці, навколишньому середовищі, географії, гуманітарних науках, безпеки, науці і техніці;
– *комерційні та громадські інформаційні служби* – поширені, оприлюднені, друковані новини поточних міжнародних, регіональних і локальних подій;
– *архіви (бібліотеки) і дослідницькі центри* – друковані документи і цифрові бази даних по ряду питань таких, як знання і навички інформаційного пошуку;
– *індивідуальна і групова (інформація)* – рукописна, мальована, опублікована, друкована або поширена інформація (наприклад мистецтво, графіті, листівки, постери або веб-сайти).

Інколи розвіддані з відкритих джерел не лише не відрізняються від таємниць, а часто перевершують секретну інформацію за цінністю. Цінність розвідданих визначається низкою характеристик, серед яких наступні [8]:

- *оперативність,* коли в якій-небудь точці планети вибухає криза, а можливості роз-відки у даному регіоні невеликі, то аналітики розвідслужб і ті, хто формує політику держави частіше вмикають телевізор або шукають інформацію в Інтернеті.
- *об'єм* – блогерів, журналістів, експертів, науковців та інших обізнаних людей навага-то більше ніж кадрових розвідників. Два або три професіональних розвідника з хорошою агентурною мережею звичайно переважають сотню журналістів у можливостях доступу до таємної інформації. Проте, грамотно скомпоновані фрагменті інформації, зібрані з відкритих джерел, часто можуть бути більш значущими ніж розвідувальні звіти.
- *якість* – у роботі розвідслужб виникають ситуації, коли звіти готуються на основі газетних вирізок та сфабрикованої інформації. У порівнянні з такими звітами, інформація з відкритих джерел незаплямована неправдою.
- *ясність* – у випадку відкритої інформації надійність відкритих джерел бу-ває як ясною, так і неясною. Ступінь надійності таємно здобутої інформації неясна майже завжди.

- *легкість використання* – таємниці, приховані грифами секретності та спеціальними програмами доступу, досить важко передати особам, що приймають рішення і, навіть, колегам-розвідникам. З даними OSINT може ознайомитись будь-яка посадова особа.
- *вартість* – розвідувальний супутник, розробка, запуск та утримування якого коштують мільярди доларів, фотографує дах заводу, де виготовляється озброєння, або корпус підводного човна. Іноземний журнал, передплата на який коштує 100 дол., може містити фотографії, зроблені в цеху заводу або відсіку підводного човна.

Розглядаючи потенційні можливості, роль та цінність OSINT, виникають певні помилкові судження. Одне з них полягає у тому, що інформація, отримана з відкритих джерел, за своєю цінністю не переважає інформацію з газет та теленовин. Насправді, OSIF отримується з різноманітних джерел, і у своїй комплексності має досить багато нюансів [9]. Інше помилкове твердження – аналітики розвідки віддають перевагу Інтернету, як відкритому джерелу. Згідно результатів, опублікованих у 2003 році, лише 3-5% здобутої інформації припадає на інтернет-ресурси. Також не є вірним твердження, що OSIF є безкоштовною. Розвідслужбам, як і іншим споживачам інформації, потрібно платити за доступ до певних джерел [4].

Проте, існує застереження – надмірна залежність від конкретного джерела (надмірна довіра якомусь одному джерелу). Невелика кількість інформації з певного джерела може бути отримана і поширена багатьма іншими джерелами. «Тиражування» одного конкретного повідомлення різними інформагенціями створює видимість «розмаїття» джерел. Якщо ця інформація циклічно анонсується, починає «множитись» проблема , оскільки кожне нове повідомлення «роздуває» початковий стан речей [9]. Звідси виникає проблема достовірності інформації та надійності джерела, особливо в Інтернеті. Для прикладу, досить часто ініціатор «зливу» певної інформації, бажаючи залишитись невідомим, використовує метод «легендування» джерела. Найбільш розповсюджена його технологія для замовних матеріалів – анонімна передача чи продаж в «незалежний» інформаційно-аналітичний центр, який далі розповсюджує цю інформацію через посередника в якомусь виданні. Далі вже журналісти відомих ЗМІ готують замовний матеріал, посилаючись на це видання. Інформація отримує видимість надійності, так як багато разів відтворювалася. Виникає ефект так званої «інформаційної хвилі» [3].

У сучасному глобалізованому світі через послаблення впливу просторово-часового фактору стає дедалі важче приховати свої таємниці, тому аналітикам розвідслужб за допомогою OSINT краще вдається забезпечити осіб, що приймають рішення (як в політиці, так і в бізнесі) відповідною інформацією. Поєднання OSINT з іншими видами розвідки та використання різних методів добування інформації (наприклад, data mining, web mining) формує інформаційний продукт високої якості, що підвищує ефективність та результативність процесу прийняття рішень.

1. *http://www.szru.gov.ua/article.php?lang=ua&root=12&item=205&page=1–Служба зовнішньої розвідки України (Матеріали комплексного огляду сектору безпеки України).*
2. *http://strateger.net/model_osint_otkritie_istochniki_v_mire_razvedki– Strategium: Политическое Экспертное Сообщество (Модель OSINT. Открытые источники в мире разведки).*
3. *http://www.amulet-group.ru/page.htm?id=865– А.Григорьев, О некоторых методах проверки достоверности информации из открытых источников.*
4. *www.fas.org/sgp/crs/intel/RL34270.pdf– Open Source Intelligence (OSINT): Issues for Congress, December 5, 2007.*
5. *http://information-retrieval.info/docs/NATO-OSINT.html–NATO Open Source Intelligence Reader (2002).*
6. *www.fas.org/irp/doddir/army/fmi2-22-9.pdf– Open source intelligence (Headquarters,Department of the Army).*
7. *http://information-retrieval.info/docs/NATO-OSINT.html –NATO Open Source Intelligence Handbook (2001).*
8. *https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/Vol49no2/reexamining_the_distinction_3.htm– Central Intelligence Agency (Reexamining the Distinction Between Open Information and Secrets).*
9. *http://www.iar-gwu.org/node/253– International affairs review (The Future of Open Source Intelligence).*