ЗАГАЛЬНОТЕОРЕТИЧНІ ПРОБЛЕМИ ДЕРЖАВИ ТА ПРАВА

УДК 327.004.738.52
DOI https://doi.org/10.32850/2414-4207.2019.11-1.01

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ВИКОРИСТАННЯ РОЗВІДКИ З ВІДКРИТИХ ДЖЕРЕЛ ІНФОРМАЦІЇ (OSINT) В ДІЯЛЬНОСТІ РОЗВІДУВАЛЬНИХ СЛУЖБ ЄВРОПЕЙСЬКИХ КРАЇН

Бурба Василь Васильович,
кандидат юридичних наук, доцент,
професор СК-4
(Навчально-науковий інститут
перепідготовки та підвищення
кваліфікації кадрів
Служби безпеки України,
м. Київ, Україна)

Стаття присвячена аналізу досвіду організації розвідки з відкритих джерел інформації в розвідувальних службах окремих європейських країн.

Проведений аналіз засвідчив, що розвідка на основі аналізу відкритих джерел інформації є невід'ємною частиною діяльності розвідувальних органів європейських країн. Характерною особливістю застосування цього методу є поєднання OSINT з іншими видами розвідки та використання різних методів добування інформації, що значно підвищує ефективність та результативність процесу прийняття управлінських рішень.

Розвідувальна діяльність із використанням відкритих джерел збільшує можливості спеціальних служб, але в її роботі є чотири критичні компоненти, на які необхідно звернути увагу: джерела, програмне забезпечення, послуги та аналіз. Їх цінність завжди зіставляється з якістю розвідувальної інформації.

Насамперед, варто зазначити, що кількість джерел інформації та її об'єми в OSINT є незрівнянно вищими, ніж у результаті її отримання оперативним шляхом, що вимагає застосування спеціальних автоматизованих комплексів обробки інформації та розробки відповідного програмного забезпечення.

Розвиток інформаційних технологій, збільшення інформаційних потоків зумовили зростання ролі OSINT у розвідувальній діяльності спеціальних служб. Зазначається, що аналіз відкритих джерел інформації проводиться практично всіма європейськими спеціальними службами, однак організована ця діяльність у різних країнах по-різному. Найбільшу складність у процесі розвідувальної діяльності на основі аналізу відкритих джерел інформації зумовлюють широкі можливості проведення спеціальних операцій щодо дезінформації.

Ключові слова: розвідка, інформаційні ресурси, бази даних, програмне забезпечення.

ORGANIZATIONAL AND LEGAL FRAMEWORK OF USING THE OPEN SOURCE INTELLIGENCE (OSINT) IN THE OPERATION OF INTELLIGENCE AGENCIES OF THE EUROPEAN COUNTRIES

Burba Vasyl Vasylovych,
Candidate of Juridical Sciences,
Associate Professor,
Professor of CK-4
(Scientific and Research Institute
of Retraining and Advanced Training
of the Personnel of the Security Service
of Ukraine, Kyiv, Ukraine)

The concept of open source intelligence is quite common today – it is widely used to describe one of the areas of activity of the vast majority of special services in the world. There is also a considerable amount of specialized research on the development of the latest intelligence search tools on the Internet. Computer intelligence covers the collection and processing of information that is conducted to support decision-making in the area of national interests, solely from open sources. The article is devoted to the analysis of the experience of the organization of open source intelligence in the intelligence services of some European countries.

The analysis showed that intelligence based on open source analysis is an integral part of the activities of intelligence agencies in European countries. A characteristic feature of this method is the combination of OSINT with other types of intelligence and the use of different methods of information retrieval, which greatly improves the efficiency and effectiveness of the decision-making process.

Open source intelligence increases the capacity of special services, but there are four critical components that need to be addressed: sources, software, services, and analysis. Their value is always compared to the quality of intelligence.

First of all, it should be noted that the number of sources of information and its volume in OSINT is incomparably higher than as a result of its prompt receipt, which requires the use of specialized automated complexes of information processing and software development.

The development of information technology and the increase in information flows have led to an increase in the role of OSINT in the intelligence activities of special services. It is noted that the analysis of open sources of information is carried out by virtually all European special services, but organized in different countries in different ways. The greatest difficulty in intelligence activities based on the analysis of open sources of information is the wide possibility of special operations on misinformation.

Key words: intelligence, information resources, databases, software.

Актуальність теми дослідження. Поняття розвідки з відкритих джерел інформації нині є досить усталеним, воно широко використовується для характеристики одного з напрямів діяльності більшості спеціальних служб світу. Також є значна кількість спеціальних досліджень, присвячених розробці новітнього інструментарію пошуку розвідувальної інформації в мережі Інтернет. Розвідка в комп'ютерних мережах охоплює процедури збору й обробки інформації, які проводяться з метою підтримки прийняття рішень у сфері забезпечення національних інтересів, виключно з відкритих джерел, більшість з яких є оверлейними. До основних цілей та завдань, які ставляться перед цим видом розвідки в процесі забезпечення інформаційної підтримки прийняття стратегічних рішень, належать:

– збір та своєчасне надання споживачам інформації різнопланового характеру, що має відношення до питань забезпечення національної безпеки;

– виявлення ризиків і загроз, що можуть перешкодити оборонному та соціально-економічному розвитку країни;

– знаходження інформації, що сприяє отриманню конкурентних переваг країни на міжнародних ринках, та визначення основних об'єктів та суб'єктів міждержавного середовища, а також виявлення їх важливих взаємозв'язків.

Важливим напрямом удосконалення роботи розвідувальних органів є створення ефективної системи отримання інформації з відкритих джерел (подібні системи створені у всіх розвідках провідних країн 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 із цим, як свідчить практика розвідувальної діяльності, ефективна робота такої системи є для вищих посадових осіб держави видимою якісною характеристикою щоденних зусиль 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].

Відкриті джерела інформації досить ретельно аналізуються у всіх країнах із розвиненими розвідувальними службами, однак організована ця діяльність у різних країнах по-різному.

Аналіз останніх публікацій. Військова доктрина США «Field Manual Interim № 2-22.9» акцентує на тому, що основною відмінністю OSINT від інших видів розвідки є те, що в її основі лежать джерело, інформація та способи їх збору, а не певна категорія технічних або людських ресурсів [2].

Досить слушною є думка авторів спеціального монографічного дослідження Nihad A. Hassan, Rami Hijazi, які зазначають, що для всіх методологій збору інформації з відкритих джерел, особливо для OSINT, характерними є проблеми такого характеру:

– аналіз величезного об'єму неструктурованої інформації вимагає застосування новітнього спеціального програмного забезпечення, розробка якого вимагає значних коштів і людських ресурсів;

– надійність джерел часто не відповідає потребам розвідки, до того ж нині в багатьох країнах стає дедалі більш поширеною практика витоку неточної інформації, що спеціально призначена для системи OSINT;

– оцінка обробленої автоматизованими системами інформації в подальшому вимагає значних витрат людського інтелекту і лише після опрацювання вузькопрофільними експертами її можна передати замовнику [3, с. 16–17].

Heather J. Williams, Ilana Blum підкреслюють, що лише незначна частина отриманої завдяки застосуванню OSINT може слугувати як релевантна інформація. Перетворення неструктурованої розвідувальної інформації на звіти для політичного керівництва держави має пройти стадію перевірки законності та надійності підсумкового документа. У цьому плані розвідка з відкритих джерел інформації потребує розробки новітніх, більш адекватних спеціальних методик [4, с. 12].

Açar, K.V. звертає увагу на раніше недосліджений аспект застосування методик збору розвідувальної інформації з відкритих джерел, що пов'язаний із масовим їх використанням як державними спецслужбами, так і приватним сектором. Кінцева інформація не має містити інформацію компрометуючого змісту для конкретної людини, оскільки вона має досить сумнівний юридичний характер. Інакше вона перетворюються на «бомбу повільної дії», внаслідок вибуху якої буде завдано значної

шкоди не лише окремій особі, але й суспільству загалом. Тому проблема потребує широкої дискусії за участі науковців та політиків [5].

Одним з основних факторів, який суттєво стримує ефективне функціонування створюваної згідно з Системою забезпечення інформаційної безпеки Міністерства оборони (МО) України та Збройних сил (ЗС) України, є відсутність на озброєнні відповідних підрозділів органів військового управління новітніх спеціалізованих програмних та (або) апаратно-програмних засобів добування, обробки, узагальнення та аналізу контентного забарвлення інформації про потенційні загрози інформаційній безпеці держави у воєнній сфері, за результатами моніторингу інформації із СМ. Авторським колективом на чолі з професором І. Грабарем розроблено автоматизовану систему контент-моніторингу та контент-аналізу соціальних інтернет-сервісів. Вона базується на принципах воєнно-технічного аналізу та орієнтується на використання сучасних інформаційних технологій. Розроблені програмні компоненти цієї системи рекомендовано застосовувати на постах OSINT-розвідки військових частин інформаційно-психологічних операцій [6].

Метою статті є аналіз європейського досвіду використання розвідувальними службами європейських країн інформації з відкритих джерел (OSINT).

Результати дослідження. Основоположником терміна «розвідка з відкритих джерел» (Open Source INTelligence – OSINT) вважається розвідувальне співтовариство США, яке почало його активне його використання з лютого 1941 р. (створення Інформаційної служби закордонного віщання – Foreign Broadcast Information Service – FBIS) [7]. Варто зазначити, що термін «розвідка з відкритих джерел» досить часто в зарубіжних джерелах є рівнозначним із терміном «конкурентна розвідка» (competitive intelligence) та «бізнес-розвідка» (business intelligence) [8].

Бельгія. Окремої нормативної бази, яка регламентує діяльність OSINT, на загальнодержавному рівні в Бельгії не існує. Разом із цим створення підрозділу, штат і категорії особового складу визначені відповідними відомчими наказами, які мають закритий характер. Підрозділ організаційно входить до складу Штабу Оборони Бельгії – Головної служби розвідки та безпеки (Service Général du Renseignement et de la Sécurité /SGRS/). Напрями діяльності та завдання підрозділу OSINT визначаються в плані збору інформації, який розробляється на підставі щорічного головного плану розвідки (затверджується урядом) та пріоритетних розвідувальних завдань. На підставі згаданого плану збору інформації підрозділ OSINT розробляє тематику огляду міжнародної преси, передплату газет, спеціалізованих та періодичних видань, передплату на доступ до спеціалізованих баз даних, тематику та спрямованість моніторингу оперативних новин. Крім цього, тематика огляду преси та моніторингу новин може змінюватись та доповнюватись (корегуватись) протягом року відповідно до розвитку обстановки у світі.

Підрозділ розвідки з відкритих джерел має загальну чисельність 7 осіб. Щорічно отримує та готує доповіді (відповіді) на більше 1500 різноманітних запитів на інформацію; Бюджет підрозділу OSINT на рік становить близько 650 000 євро на доступ до спеціалізованих баз даних. Ця сума не враховує передплату на газети, журнали та інші періодичні видання.

Як одну з основних баз даних інформації підрозділ OSINT використовує FACTIVA, доступ до якої за рік коштує 25 000 євро. Раніше підрозділ використовував французьку Lexis Nexis, яка оцінюється як менш спроможна порівняно з FACTIVA.

Вибір баз даних для оформлення й оплати доступу здійснюється на підставі пропозицій підрозділу OSINT із застосуванням загальних правил щодо проведення тендерів, які діють у збройних силах. З огляду на доповіді фахівців підрозділу, близько 80% потрібної для них інформації в інтернеті можна отримати лише на платній основі.

Республіка Болгарія. Окремої нормативної бази, яка б регламентувала діяльність системи OSINT, у РБ немає. Зазначений вид розвідувальної діяльності здійснюється спеціальними службами РБ у рамках Закону «Про Міністерство внутрішніх справ», Закону РБ «Про спеціальні розвідувальні засоби», а також відомчих нормативних актів. Підрозділи, які безпосередньо займаються добуванням розвідувальної інформації з відкритих джерел, структурно входять до таких спеціальних служб РБ:

– у Національній розвідувальній службі РБ – дирекція «Інформації і аналізу»;
– у Національній службі охорони (НСО) – інформаційно-аналітична група;
– у Державній агенції «Національна безпека» – дирекція бюро «Координація і інформаційно-аналітична діяльність»;
– у Службі «Військова інформація» МО РБ (СВІ) – дирекція «Аналізу і прогнозу».

У країні розроблені і використовуються програмні продукти, що дають змогу здійснювати моніторинг джерел інформації, як це декларується в інтересах бізнесу – DAXY Global і DAXY007. Системи дають змогу відслідковувати в автоматичному режимі появу визначених за тематикою повідомлень, осіб, фірм тощо. Є дані, що нині з боку адміністрації США активно вживаються заходи щодо залучення з числа болгарських громадян так званих «агентів для роботи з відкритими джерелами». Пріоритет надається колишнім розвідникам, експертам, представникам ЗМІ. Їх робота полягає в перегляді сайтів, газет, повідомлень інформаційних агенцій, телебачення, радіо і спеціалізованих публікацій із метою збору важливої інформації.

За наявними даними, спецслужбами РБ із відкритих джерел добувається від 65% до 85% розвідувальної інформації.

Королівство Великобританія. Робота з відкритими джерелами у країні має глобальний характер і координується на найвищому політичному рівні. Відповідні підрозділи є у всіх спеціальних службах країни, а також у багатьох державних установах, а тому доцільно розглянути лише нормативне забезпечення її діяльності та завдання, що вирішуються.

Відповідно до ААР-6, у ВР Великобританії застосовується таке визначення: «РІВД – це інформація з джерел, до яких є публічний доступ, а також інша нетаємна інформація, яка має певні обмеження для поширення та доступу серед широкого загалу». Діяльність системи РІВД регламентується законом «Про розвідувальні служби» (Intelligence Services Act) від 1994 р. зі змінами та доповненнями від 2001 р., а також відомчим таємним Положенням про ВР Великобританії. Крім того, застосовуються вказівки Об'єднаного розвідувального комітету Великобританії та положення відповідних стандартів НАТО.

Система добування інформації з відкритих джерел у воєнній розвідці (ВР) Великобританії є складовою частиною загальної системи МО Великобританії, яку очолює Генеральний директор інформаційного департаменту МО Великобританії. У складі департаменту є підрозділ чисельністю до 25 осіб, який займається питаннями інформаційного забезпечення з відкритих джерел. Зазначений підрозділ діє в тісній взаємодії з ВР Великобританії. У структурі Штабу розвідки МО (ШРМО) Великобританії створений відділ у складі 4 осіб, який відповідає за організацію та забезпечення роботи з розвідувальною інформацією з відкритих джерел (РІВД). Відділ входить до складу Управління стратегічного планування добування розвідувальної інформації, яке підпорядковується Генеральному директору воєнної розвідки з оперативних питань.

Головним завданням системи РІВД є забезпечення необхідною та своєчасною інформацією інформаційно-аналітичних підрозділів ВР Великобританії. Напрями моніторингу джерел інформації визначаються пріоритетами та завданнями, які стоять перед інформаційно-аналітичними підрозділами ВР Великобританії.

Іспанія. Законодавча база, що регламентує діяльність підрозділів розвідки з відкритих джерел: Закон № 23/2006 від 7 липня 2006 р., яким внесені зміни до Закону про інтелектуальну власність, затвердженого Королівським декретом № 1/1996 від 12 квітня 1996 р.; Королівський декрет № 1/1996 від 12 квітня 1996 р., яким затверджується тест Закону про інтелектуальну власність; Закон про захист даних персонального характеру № 15/1999 від 13 грудня 1999 р.; Нормативні акти щодо регламентації OSINT у рамках НАТО та ЄС. Відповідні підрозділи функціонують у всіх спеціальних службах, а також у більшості міністерств та відомств.

У структурі Розвідувального центру Збройних сил Іспанії (ЗЦ ЗС) є Група по роботі з відкритими джерелами інформації (OSINT) з чисельністю до 7 осіб. Завдання Групи – отримання необхідної інформації від відкритих джерел, якої на постійній основі або періодично потребують аналітичні підрозділи РЦ ЗС, інші державні установи або деякі країни-партнери, для задоволення як специфічних завдань, згідно з програмою здобуття розвідувальної інформації, так і завдань згідно з інформаційними запитами. Діяльність Групи здійснюється щоденно протягом року з таким розрахунком, щоб аналітики отримували продукт на початку робочого дня. У разі необхідності, діяльність робочої групи здійснюється 24 години на добу. Як підрозділ здобуття інформації Група є частиною органу РЦ ЗС, відповідального за систему тривоги та супроводження кризи, координує свою діяльність через орган координації здобуття та управління інформаційними запитами (CCIRM) й організовує свою роботу за трьома напрямами: інформаційні агентства; зони операцій; решта інформації. Кожен член групи OSINT має чітко визначений напрям роботи та тематику відповідальності.

Технічні засоби, що застосовуються («Software» програм «ad-hoc» та «Hardware») необхідні для: анонімного доступу в Інтернет через «praxis»; реалізації ручного або автоматичного пошуку, вибору та здобуття текстової інформації та зображень в інтернеті як у формі запрограмованій, так і у вибірковій; ручного або автоматичного здобуття аудіо- та відеосигналів, які поширюються телевізійними станціями або представлені на вебсторінках, а також трансформації аудіосигналів у текст.

Пошук є запрограмованим і має дві форми: щоденний та щомісячний. Щоденний пошук – це узагальнення інформації щодо зон, де розгорнуті контингенти Збройних сил Іспанії та зон спеціального інтересу відповідно до форми щоденного отримання інформації через інтернет. Щомісячний пошук – це здобуття інформації відповідно до завдань PROGINT. У кожному щомісячному циклі здобувається інформація відповідно до всіх визначених завдань, з яких три перші тижня приділяються сфері пріоритетного інтересу для розвідки (AIPI), четвертий тиждень – іншим сферам інтересу для розвідки (OAII), а всередині їх – у порядку пріоритетності. Може також здійснюватися пошук відповідно до запитів, отриманих від CCIRM.

Італія. Діяльність розвідувальних органів та спеціальних служб зі збору та обробки інформації з відкритих джерел здійснюється відповідно до закону № 124 від 3 серпня 2007 р. щодо «Системи розвідки та безпеки Італійської Республіки та нового порядку забезпечення державної таємниці». 7 серпня 2012 р. набув чинності новий Закон № 133, який передбачає внесення змін до вищезазначеного закону. Доповнення складається із 12 статей, які передбачають зміни до повноважень та завдань парламентського комітету з питань безпеки, дотримання державної таємниці, функціонування та підпорядкування спецслужб.

Інформація стосовно структури підрозділів OSINT італійських секретних служб та нормативної бази, яка регламентує діяльність цих підрозділів, має закритий характер, оскільки, на думку керівництва секретних служб Італії, аналіз діяльності OSINT може привести до розкриття змісту конкретних аспектів оперативної діяльності.

У складі ЗС Італії є Управління інформації та безпеки (УІБ) ГШО, яке має завданням ведення розвідувально-інформаційної діяльності з метою захисту розташування та діяльності військових підрозділів ЗС Італії за кордоном. У складі Управління відсутній єдиний інформаційно-аналітичний підрозділ, а тому, відповідно до визначених завдань, кожен підрозділ УІБ готує інформаційно-аналітичні матеріали, призначені для інформування військового керівництва виключно за своїм напрямом.

Міжвидовий розвідувальний центр, який організаційно входить до складу УІБ, безпосередньо здійснює інформаційне забезпечення операцій, що проводяться за межами національної території, має в підпорядкуванні розвідувальні відділи видів ЗС Італії та тісно співпрацює із Службою розвідки управління операцій Вищого міжвидового оперативного командування (COI). Завданнями згаданих відділів є збір, обробка та передача до УІБ розвідувальної інформації, в тому числі з відкритих джерел.

У цивільних органах, згідно з законом № 124, органом, який безпосередньо координує діяльність секретних служб Італії, є Департамент розвідки та безпеки при Раді Міністрів Італії, до функціональних обов'язків якого, у тому числі, входить підготовка інформаційно-аналітичних документів, інформування та надання рекомендацій вищому державному керівництву країни на підставі отриманої розвідувальної інформації, що надходить від відповідних інформаційних підрозділів Агентства розвідки та зовнішньої безпеки й Агентства розвідки та внутрішньої безпеки, а також спеціальних органів Військ карабінерів, Фінансової гвардії, Державної поліції та ЗС Італії.

Під час підготовки доповідей та відпрацювання аналітичних матеріалів спеціальні служби Італії використовують до 60% інформації з відкритих джерел із метою порівняння, спростування або підтвердження їх достовірності.

Республіка Польща. Окремої нормативної бази, яка регламентує діяльність спеціальних служб та інституцій Польщі по роботі з відкритими джерелами інформації (OSINT), не існує, кожна служба організує цю діяльність у межах чинного законодавства та компетенції служб.

Окремі структури (принаймні на рівні управління OSINT) для роботи з відкритими джерелами інформації в польських державних розвідувальних структурах нині відсутні. Однак варто розуміти, що OSINT як метод добування використовується розвідувальними підрозділами усіх рівнів відповідно до свого технічного оснащення та можливостей, а OSINT у глобальному розумінні здійснюється інформаційно-аналітичними підрозділами управлінь служб та інституцій. Серед основних особливостей побудови системи інформаційно-аналітичного забезпечення та організації її роботи є те, що розвідувальні органи країни широко використовують органи стратегічного аналізу та прогнозування розвитку військово-політичної обстановки. Ці органи спираються, насамперед, на налагоджену систему отримання та обробки відкритих джерел інформації: з власних підрозділів та експертних центрів; на безоплатній основі з аналітичних центрів міжнародних організацій у структурі ЄС та НАТО, а також з обміну з аналогічних інституцій країн-союзників; на платній основі в комерційних аналітичних центрах, власних чи країн-союзників. Прикладом може бути використання Міністерством закордонних справ РП послуг Нью-Йоркського центру The Economist Intelligence Unit. Так, із грудня 2010 р. МЗС РП укладає річні контракти на поставку аналітичних матеріалів із питань міжнародних політичних, соціальних та економічних стосунків, що вважається альтернативним джерелом інформації, а також коротко- та довгострокові політико-економічні прогнози (2, 4 і 25 років) розвитку ситуації в 82 країнах світу.

Прикладом простого та ефективного програмного забезпечення data mining може слугувати Chost Miner (3,0), розроблене Кафедрою інформатики Університету

в Торуню, яке було комерціалізоване фірмою FQS Poland. Chost Miner складається з двох основних елементів: інструмент для створення моделі знань, що буде підставою для подальшого аналізу та прийняття рішень; інструмент, який полегшує аналізування даних, відображення та використання.

Федеративна Республіка Німеччина. У ФРН реалізується низка таємних програм, які передбачають розбудову можливостей правоохоронних структур та спецслужб країни добувати та аналізувати інформацію у відкритих інформаційних системах в інтересах національної безпеки.

Федеральна розвідувальна служба (Bundesnachrichtendienst) країни реалізує Концепцію «Стратегічна технологічна ініціатива» (Strategische Initiative Technik), яка включає 26 проектів та передбачає розбудову апаратного та програмного забезпечення для покращення ведення електронної розвідки та, зокрема, моніторингу соціальних мереж. Розробка техніко-економічного обґрунтування Концепції була розпочата ФРС ще у 2013 р.

Федеральне міністерство оборони ФРН реалізує проект «Отримання інформації з відкритих джерел» (Wissenserschließung aus offenen Quellen, WeroQ), який передбачає створення системи автоматизованого аналізу відкритих джерел інформації в цілях воєнної безпеки країни. Головний підрядник – Науково-дослідний інститут зв'язку, обробки інформації та ергономіки (Forschungsinstitut für Kommunikation, Informationsverarbeitung und Ergonomie, FhG FKIE), субпідрядник – компанія «IBM» (США).

Висновки. Проведений аналіз засвідчив, що розвідка на основі аналізу відкритих джерел інформації є невід'ємною частиною діяльності розвідувальних органів європейських країн. Характерною особливістю застосування цього методу є поєднання OSINT з іншими видами розвідки та використання різних методів добування інформації, що значно підвищує ефективність та результативність процесу прийняття управлінських рішень.

Розвідувальна діяльність із використанням відкритих джерел збільшує можливості спеціальних служб, але в її роботі є чотири критичних компоненти, на які необхідно звернути увагу: джерела, програмне забезпечення, послуги та аналіз. Їх цінність завжди зіставляється з якістю розвідувальної інформації.

Насамперед, варто зазначити, що кількість джерел інформації та її об'єми в OSINT є незрівнянно вищими, ніж у результаті її отримання оперативним шляхом, що вимагає застосування спеціальних автоматизованих комплексів обробки інформації та розробки відповідного програмного забезпечення. Головною загрозою для ведення розвідувальної діяльності з використанням відкритих джерел було, є та залишатиметься їх широке використання для проведення спеціальних заходів дезінформації.

Список використаних джерел:

1. Матеріали Комплексного огляду сектору безпеки України. URL: http://www.szru.gov.ua/article.php?lang=ua&root=12&item=205&page=1.

2. Open Source Intelligence, U.S. Army Field Manual Interim FMI 2-22.9, December 2006. URL: www.fas.org/irp/doddir/army/fmi2-22-9.pdf.

3. Nihad A. Hassan, Rami Hijazi. (2018). Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence.

4. Heather J. Williams, Ilana Blum. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. Library of Congress Control Number: 2018943942.

5. Açar, K.V. (2018). OSINT by Crowd-Sourcing: A Theoretical Model for Online Child Abuse Investigations/ *International Journal of Cyber Criminology*. Vol. 12(1): 206–229.1467897 Publisher & Editor-in-Chief. K. Jaishankar.

6. Грабар І.Г. Безпекова синергетика: кібернетичний та інформаційний аспекти : монографія / І.Г. Грабар, Р.В. Грищук, К.В. Молодецька. Житомир : ЖНАЕУ, 2019. 280 с.

7. Open Source Intelligence. FMI 2-22.9. December 2006. Federation of American Scientists. URL: http://www.fas.org/irp/doddir/army/fmi2-22-9.pdf.

8. Akhgar, B., & Wells, D. (2018). Critical success factors for OSINT Driven Situational Awareness. *European Law Enforcement Research Bulletin*. #18.