DOI: 10.18372/2307-9061.64.16895
УДК 340:355.4(045)

Н. В. Жмур,
кандидат юридичних наук
ORCID ID: https://orcid.org/0000-0001-5462-4482

М. П. Землянікіна,
бакалавр права

ІСТОРІЯ СТАНОВЛЕННЯ ТА СУЧАСНИЙ СТАН ТЕХНОЛОГІЇ ПОШУКУ ІНФОРМАЦІЇ OSINT

Національний авіаційний університет
проспект Любомира Гузара, 1, 03680, Київ, Україна
E-mails: nataliia.zhmur@npp.nau.edu.ua, 5654340@stud.nau.edu.ua

Метою *статті є визначення поняття OSINT як технології пошуку та використання інформації з відкритих джерел, розкриття значення, цінності та сутності такого поняття як «розвідка з відкритих джерел», а також дослідження історичних аспектів і надання уявлення про перспективи використання технології OSINT.* ***Методи дослідження:*** *документального аналізу і синтезу, порівняльного аналізу, об'єктивної істини, пізнавально-аналітичний, міжгалузевий метод юридичних досліджень, історичний, пізнавально-аналітичний та ін.* ***Результати:*** *звернення до історичних етапів становлення OSINT надасть можливість вдосконалити технологію пошуку та використання інформації з відкритих джерел без порушення норм законодавства.* ***Обговорення:*** *на підставі досліджених даних проаналізовані історичні аспекти розвитку OSINT та перспективи сучасного використання технології, як одного із способів отримання розвідувальної інформації.*

Ключові слова: *розвідка; відкриті джерела інформації; законність; пошук інформації; кіберпростір; аналітика.*

Постановка проблеми та її актуальність. Сьогодні людство є свідком активного переходу від індустріального суспільства до інформаційного. В провідних країнах постійно з'являються сучасні способи добування розвідувальної інформації, наразі все більше інформації можливо знайти у відкритих джерелах.

Діяльність з отримання розвідувальної інформації з відкритих джерел кіберпростору отримала назву OSINT – це акронім Open Source INTelligence чи відкриті джерела розвідки.

Через стрімкий розвиток сучасних інформаційних технологій ця технологія набуває популярності й у відповідних силових структурах України.

Особливу актуальність дана технологія в Україні отримала після повномасштабного вторгнення росії, оскільки початкова інформація з відкритих джерел після певного аналізу і опрацювання може стати цінним знанням, особливо в умовах війни.

Фактично, OSINT – це та ж розвідка, але на заміну величезному людському ресурсу приходять сучасні технології, штучний інтелект, який допомагає швидко дізнатися про те, що, як і де відбувається.

Аналіз досліджень і публікацій з проблеми. Дослідженням технології OSINT приділяли увагу такі науковці як: О.О. Кожушко, В.В. Сумська, А.М. Онупрієнко, Є.Б. Тихомирова, В.Л. Федоренко, Н.Ф. Ржевська, О.В. Минько, О.Ю. Іохов, К.В. Власов, І.П. Мігус, Р.М. Мацкевич, В.В. Ровний та інші.

Мета статті полягає в комплексному дослідженні механізму отримання розвідувальної інформації з відкритих джерел у історичному та сучасному стані.

Виклад основного матеріалу. В XXI столітті спостерігається тенденція стрімкого розвитку інформаційних технологій. Сьогодні, на просторах інтернету можна знайти майже будь-які дані на будь-яку тематику. Тому роль та цінність інформації зростає щодня.

В першу чергу, варто з'ясувати сутність терміну «OSINT» та історію його виникнення. Розвідка відкритих джерел (Open source intelligence, OSINT) – концепція, методологія і технологія добування без порушення законів і використання військової, політичної, економічної та іншої безпекової інформації з відкритих джерел – для підтримки прийняття рішень у сфері національної оборони і безпеки. Включає в себе, більш детально, для прикладу: забезпечення безпеки інформаційної роботи, адміністрування інформації; пошук інформації; реєстрація і облік інформації; аналіз інформації і синтез знань з різних джерел (аналітико-синтетична переробка первинної інформації, у теперішній час з обов`язковим використанням засобів Business Intelligence, Knowledge Management System, ін.); розповсюдження інформації [1].

Intelligence в узагальненій дефініції OSINT можна розуміти також не як «розвідку», а як «аналітичні документи», «аналітичну інформацію», що отримані у результаті аналітико-синтетичної обробки законно добутої первинної інформації [1].

Потрібно відрізняти OSINT (Open Source INTelligence) від OSIF (Open Source InFormation). OSIF – це дані й відомості, що циркулюють у вільно доступних медіаканалах, а OSINT – це специфічна інформація, зібрана і особливим чином структурована заради відповіді на конкретні питання [2]. Різниця полягає у тому, що проблемним завданням агентури є отримання необхідної інформації з джерел, які зазвичай не хочуть ділитись наявними даними, а проблемним завданням розвідки з відкритих джерел є необхідність достеменного осередку загальнодоступної інформації.

Важливим завданням є дослідити історію виникнення та становлення OSINTу. Достеменно невідомо дату та передумови створення даної технології, але науковці виділяють декілька етапів. Зокрема:

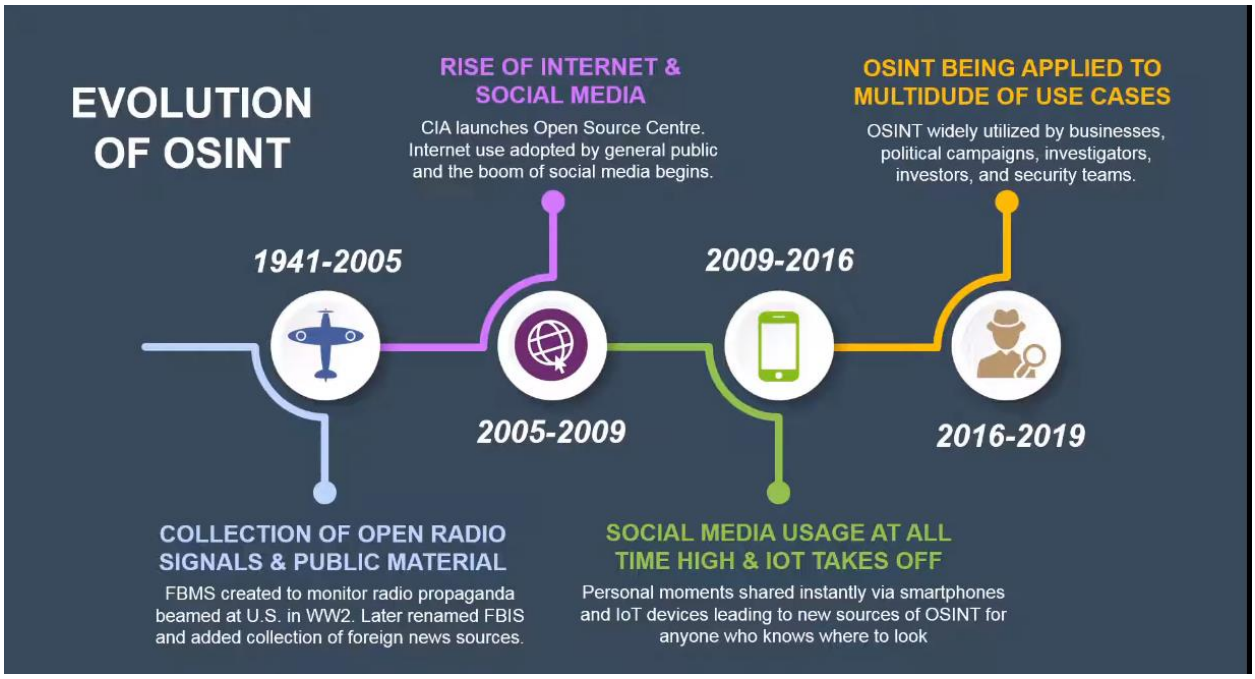
1) кінець 1941 р. – створення у Штатах Служби моніторингу зарубіжних трансляцій задля дослідження радіо програм. Результатом дослідження стало виявлення працівниками цієї служби взаємозв'язку між вартістю апельсинів у Парижі та вдалим бомбардуванням залізничних мостів;

2) 2005-2009 рр. – у США був створений центр із аналізу розвідувальних матеріалів з відкритих джерел. Відбулося це внаслідок зростання кількості інформації, що розміщувалась на просторах інтернету;

3) 2009-2016 рр. – стрімкий розвиток інтернету, його ролі та впливу на людське життя;

4) 2017 р. – сьогодення – поступове введення концепції OSINT не лише в сферу оборони, але й в інші сфери життєдіяльності людини.

У практиці розвідки не останнє місце займає JISR. Це синхронізація та інтеграція можливостей та заходів операцій та розвідки, спрямовані на надання своєчасної інформації для підтримки прийняття рішень. «Процес циклу JISR» – це комбінована функція розвідки та операцій, що вимагає широкої координації та співпраці між співтовариством на багатьох рівнях. JISR НАТО інтегрує можливості Альянсу та національних систем розвідки, спостереження та рекогносцировки (ISR), політику, процедури та системи для надання інформаційної підтримки лідерам, командирам та особам, які приймають рішення, від політичних і стратегічних сфер до тактичного рівня включно. На JISR-процес покладається місія забезпечити командира всіма специфічними даними, інформацією і ситуаційною обізнаністю, що стосується збору інформації в процесі проведення операції. Така архітектура процесу дає змогу інтегрувати наявні розвідувальні спроможності в загальну схему маневру операції. Розвідка є лише частиною операції, а пріоритети операції в цілому, місце та діяльність розвідки в підтримці операції визначає командир. JISR-процес виконується в п'ять послідовних кроків: вимоги (task), збір (collect), обробка (process), використання (exploit) і поширення (disseminate), які мають абревіатуру TCPED. Пропонуємо нижче більш детально розглянути даний процес.



Мал. 1 [2]

1. Надання «вимог» (tasking) є першим кроком JISR-процесу, який полягає в чітких вимогах до збору у вигляді інструкцій і наказів для координації та контролю JISR-засобів.

2. На цьому кроці задіюються функції персоналу штабу з управління вимогами до розвідки (IRM) та визначають оптимальні джерела розвідки з огляду на операційну необхідність, ризики застосування, обмежену наявність інструментів. Малоймовірно, що особовий склад розвідки колись матиме достатню кількість людей або ресурсів, аби задовольнити всім запитам. Ведення розвідки має бути заздалегідь спланово й організовано настільки надійно, наскільки це можливо в межах наявних обмежень. Для її успішного ведення мають бути визначені пріоритети процесу розвідки, враховуючи, що вимоги не завжди відповідають наявним спроможностям.

3. Третій крок – «обробка» (process) полягає в конвертації зібраних даних у встановлені, зручні формати, які дозволяють візуалізацію, подальше використання, зберігання і поширення оброблених даних. Головною вимогою виконання цього кроку є побудова єдиної інформаційної мережі, завдяки якій добиваються ефекту синергії, коли ефективність від сумісної дії об'єднаних у мережу сил за сукупним результатом перевищує сумарну ефективність від застосування тих же сил та засобів окремо.

4. Поширення оброблених даних в єдиній мережі є важливим для обробки даних з інших джерел розвідки, які в цей же час задіяні в цій або суміжній зоні відповідальності. Горизонтальні зв'язки сприяють поширенню розуміння, що є істотним для оптимізації застосування різних джерел розвідки. Кожне джерело у співпраці з іншими може відкоригувати власний збір даних і поліпшити якість інформації в результаті їх обробки.

5. П'ятий крок JISR-процесу – «поширення» (dissemination) включає своєчасне постачання JISR-результатів авторизованим запитувачам в необхідному форматі обумовленими каналами комунікації. Важливо, щоб поширювана ситуаційна обізнаність була стислою і наочною для уникнення переобтяження командира [5].

Необхідність використання відкритих джерел інформації в політиці та військовій сфері є безспірною. Зокрема, більшість науковців дотримуються позиції, що інформація, добута із відкритих джерел, є набагато цінішою, аніж та, що добувається секретно. Вважають, що такі джерела є більш надійними і більш корисними, ніж «секретні» джерела, оскільки останні важко перевірити на достовірність та оцінити реальну

цінність [6]. Під загальною цінністю розвідданих розуміють такі їх аспекти, як швидкість надходження, чисельність, якість, достовірність, легкість подальшого використання і вартість отримання. Нижче пропонуємо охарактеризувати кожен із наведених вище аспектів:

1) швидкість надходження. Часто трапляється так, що в певному регіоні виникає критична ситуація, а можливості розвідувальних служб є досить обмеженими. Тому представники таких служб часто у своїй роботі використовують інформацію, що знаходиться на теренах інтернету. Хоча використання такої техніки в державах, де можливості не є обмеженими і майже вся інформація добувається секретно є також доволі частим явищем, бо найбільш хвилюючі та важливі ситуації відображаються саме в новинах: на паперових носіях, в інтернеті, чи на екрані телевізорів. Тому за падінням Берлінської стіни стежили з усіх куточків світу просто з екранів телевізорів, а не за допомогою розвідки;

2) чисельність. Кількість кадрових спеціалістів розвідки є значно меншою, аніж осіб, які безпосередньо мають справу із обігом інформації: журналістів, телерепортерів, аналітиків та блогерів та ін. Звичайно, що добре підготовлений спеціаліст розвідки, може мати перевагу над не одним десятком фахівців, що були наведені вище. Однак, як показує досвід, грамотно зібрана інформація з відкритих джерел за своєю значущістю може бути цілком еквівалентні, а іноді і вища;

3) якість. Часто трапляється так, що таємні агенти надають зібрану інформацію, яка була навмисне сфабрикована ними ж або іншими особами, яким це було потрібно. Тому перевага OSINTу полягає у тому, що відкриті джерела менш завуальовані неправдивою інформацією як мінімум агентів;

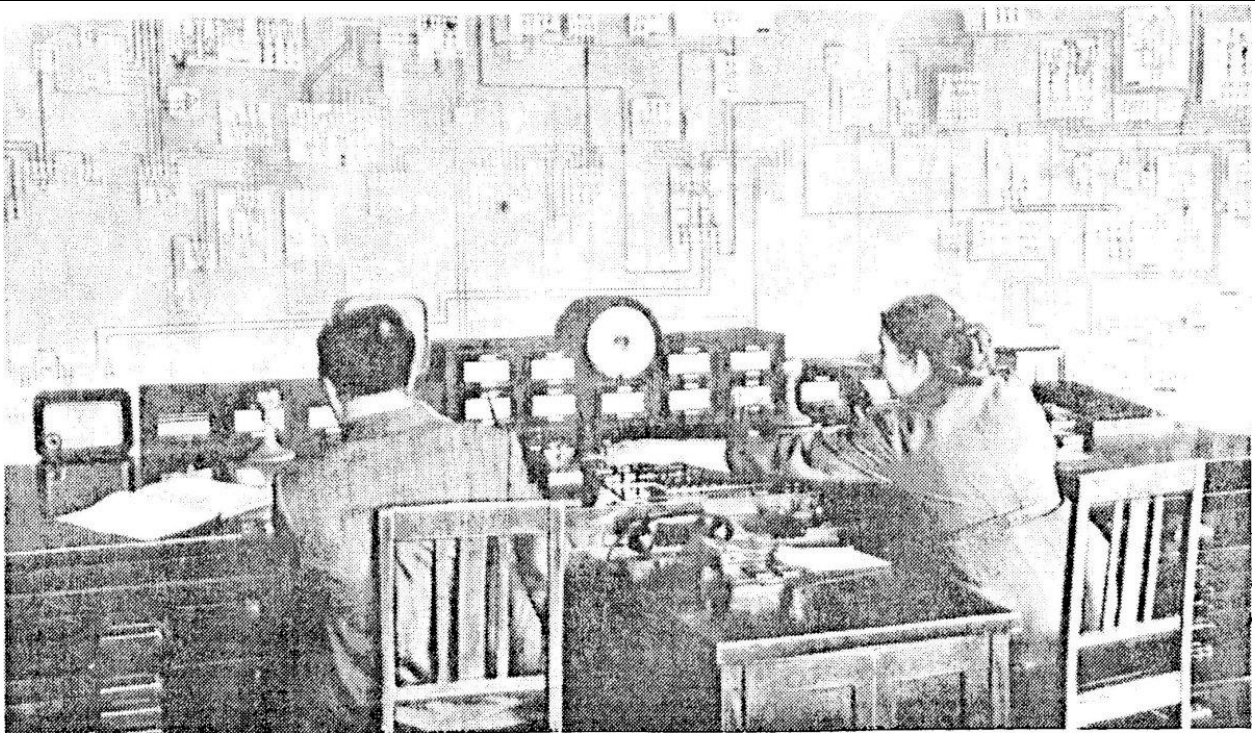
4) достовірність. Досить серйозною проблемою для аналітиків розвідки є неможливість встановити рівень достовірності добутої інформації, навіть якщо вона отримана через агентурні джерела. Розвідувальні управління різних країн світу досить ретельно охороняють та «турбуються» про джерела, які надають їм інформацію та шляхи отримання такої інформації. Тобто, можна зробити висновок, що у випадку з відкритими джерелами інформації ситуація з надійністю є зрозумілішою, оскільки надійність таємно добутої інформації для аналітиків є незрозумілою майже завжди;

5) легкість використання. Будь-які таємниці прийнято оточувати бар'єрами з грифів секретності, обмежувати та встановлювати особливих режими доступу. Все це робить надзвичайно непростим не тільки процес передачі здобутих відомостей в політичні структури, які приймають рішення, але і поширення важливих даних серед колег-розвідників, не кажучи вже про поліцію. Що ж стосується даних OSINT, то зрозуміло, що їх можна легко передавати в будь-які зацікавлені інстанції;

6) вартість. Супутник видової розвідки, що розробляється, запускається і підтримується в працездатному стані на орбіті, обходиться в мільярди доларів. Він може надати фотографії того, як виглядає дах військового заводу або корпус нового підводного човна. В той же час, у правильно обраному іноземному журналі ціною близько сотні доларів можна виявити фотографії, зняті в цехах того ж заводу або всередині того ж човна.

Деякі представники американської розвідки зазначають, що розвіддані, які здобуті агентурою, займають досить невелику частку, натомість на загальнодоступні джерела інформації вони відводять близько вісімдесяти відсотків. Різниця колосальна, але варто пам'ятати про те, що саме отримані розвідкою деталі дозволяють верифікувати здобуті дані.

В ЦРУ за радянських часів відновили на основі фотографії з журналу схему електрифікації Уралу і підприємств ядерної промисловості. Аналітики розвідки зачепилися за одне заретушоване зображення панелі моніторингу, а потім виконали величезну роботу, збираючи дані з радянських газет, журналів та звітів дипмісій. Але вирішальними виявилися знімки місцевості з розвідувальних аеростатів, тому що інакше неможливо було підтвердити правомірність висновків про розташування ліній енергопередачі і заводів [4].



Мал. 2 [4].

Окрім військової сфери та політики OSINT також активно використовується в інших сферах життєдіяльності людини. Зокрема, маркетинг, журналістика, бізнес та інші. В галузі маркетингу та бізнесу дана технологія корисна тим, що таким чином вираховується цільова аудиторія, оцінюються наявні та можливі конкуренти, переваги та ризики, а також формується концепція завдяки якій досягається головна ціль – максимальне задоволення потреб споживача, а відповідно для бізнесу – прибуток. Журналісти-ці це вигідно тим, що вони матимуть доступ до матеріалів, які допоможуть ефективно провести розслідування, яке непідконтрольне правоохоронним органам, а також для написання майбутніх статей.

Але не завжди OSINT використовується для благих цілей. Часто зловмисники застосовують дану технологію для того, щоб вчинити протизаконні дії і заподіяти шкоду іншим. Попередній аналіз дозволяє дізнатися про працівників, про клієнта, що дозволяє краще здійснити атаку. Це одна з причин, щоб обмежувати публічну інформацію про компанію. Також він активно використовується дослідниками загроз різного програмного забезпечення. Вони досліджують можливі шляхи розповсюдження шкідливих програм і перешкоджають цьому. Одним із відкритих джерел, для перевірки файлів або програм на наявність шкідливого функціоналу є virustotal.com. У користувача є можливість перевірити файл за контрольною сумою або ж завантажити його, і переконатися в його безпеці [2].

Як нам відомо, НАТО є військово-політичним союзом, який займається питаннями оборони та захисту, тому очевидним є те, що дана організація матиме безпосереднє відношення до теми нашої роботи. Зокрема, на початку 2017 року був створений новий підрозділ під назвою «Об'єднаний відділ розвідки і безпеки» (JISD). Вважають, що ця реформа є надзвичайно важливою для історії розвідки Альянсу. Межа між цивільним і військовим, між війною і миром дедалі більше розмивається. Це також робить необхідною кращу інтеграцію цивільної і військової розвідки в НАТО в єдину ефективну структуру, здатну забезпечити Північноатлантичну раду і Військовий комітет НАТО цілісною розвідувальною картиною. Ці міркування підштовхнули лідерів Альянсу до початку фундаментальної реформи розвідки НАТО на саміті

у Варшаві в липні 2016 року. Ключовим елементом цієї реформи стало створення нового підрозділу в штаб-квартирі НАТО, який складається з двох частин: розвідки (з об'єднаними напрямами цивільної і військової розвідки) і безпеки (Офіс безпеки НАТО). Так само, із розширенням ролі НАТО в протидії тероризму, Альянсу потрібне більш глибоке знання обстановки в цій сфері. Для цього було створено нову Групу розвідки з питань тероризму, яка зосередилась на забезпеченні стратегічної розвідувальної інформації з усього світу. Секція безпеки цього відділу також приділяє велику увагу тероризму. Офіс безпеки НАТО продовжує забезпечувати безпеку штаб-квартири НАТО і персоналу НАТО, залученого до виконання місій. Він також розробляє стандарти безпеки задля захисту закритої інформації і систем, і забезпечення виконання цих вимог установами НАТО, країнами-членами НАТО і країнами-партнерами. Його включення в склад нового відділу надає додаткові можливості досягнення більшої синергії в нашій роботі, особливо між розвідкою і контррозвідкою [3].

Одна з найбільш детальних інформацій щодо OSINT у НАТО викладена у збірниках «NATO Open Source Intelligence Handbook» (2006-2017 рр.) і «NATO Open Source Intelligence Reader» (2006-2017 рр.), який згідно передмови надає вичерпну інформацію та різноманітні погляди на OSINT – інформація має відношення до всіх команд НАТО, цільових груп, країнчленів, цивільно-військових комітетів і робочих груп, а також інших організацій, які можуть планувати або брати участь у спільних операціях. Третій збірник у цій групі документів НАТО, «NATO Intelligence Exploitation of the Internet» (2002 р.) застарів і посилання на нього видалене, хоча він доступний в Інтернеті на інших ресурсах [2]. Тобто, дана організація відіграє досить важливу роль в розвитку цього методу і розвідки в цілому.

Висновки. Отже, виходячи з вище наведеного можна стверджувати про те, що роль та цінність технології розвідки з відкритих джерел інформації «OSINT» є безспірною. Так як тема не є всебічно дослідженою, фахівці не можуть дійти до спільної думки з приводу питання: «Скільки ж все-таки відсотків розвідданих добувається саме з відкритих джерел інформації?». Деякі вважають, що від 35 до 95% розвідданих і при цьому частка витрат на OSINT в розвідувальному бюджеті США становить близько 1 відсотка. Інша ж думка полягає у тому, що показник є сталим і дорівнює близько 80%. Дана методика виникла відносно недавно і ще не набула широкого застосування різними країнами світу. Але вже зараз досить велика кількість вважають цю концепцію потужною та, можливо, одним із найбільш перспективних засобів розвідки на майбутнє.

Література

1. OSINT (воєнна розвідка відкритих джерел) в екосистемі зв`язаних термінів. URL: https://dss-bi.blogspot.com/2019/01/osint.html (дата звернення 02.06.2022).

2. Розвідка на основі відкритих джерел. URL: https://sidcon.com.ua/ru/osint (дата звернення 02.06.2022).

3. Адаптація розвідки НАТО для підтримки «Єдиної НАТО». URL: https://www.nato.int/docu/review/uk/articles/2017/09/08/adaptatsya-rozvdki-nato-dlya-pdtrimki-dino-nato/index.html (дата звернення 02.06.2022).

4. Бойовий OSINT. Розбираємо сучасні методи розвідки мережі. URL: https://www. guardianelinks.com/threads/boevoj-osint-razbiraem-sovremennye-metody-setevoj-razvedki.38215/ (дата звернення 02.06.2022).

5. Розвідувальний процес за поглядами воєнних фахівців НАТО. URL: https://bintel.org.ua/nukma/rozviduvalnij-proces-nato/ (дата звернення 02.06.2022).

6. Жмур Н.В. Международно-правовые стандарты защиты информации: отдельные аспекты. *Legeasi Viata.* 2014. № 2/2 (266). С. 90-93.

References

1. OSINT (voienna rozvidka vidkrytykh dzherel) v ekosystemi zviazanykh terminiv. URL: https://dss-bi.blogspot.com/2019/01/osint.html (data zvernennia 02.06.2022).

2. Rozvidka na osnovi vidkrytykh dzherel. URL: https://sidcon.com.ua/ru/osint (data zvernennya 02.06.2022).

3. Adaptatsiia rozvidky NATO dlia pidtrymky «Yedynoi NATO». URL: https://www.nato.int/docu/review/uk/articles/2017/09/08/adaptatsya-rozvdki-nato-dlya-pdtrimki-dino-nato/index.html (data zvernennia 02.06.2022).

4. Boyovyy OSINT. Rozbyrayemo suchasni metody rozvidky merezhi. URL: https://www.guardianelinks.com/threads/boevoj-osint-razbiraem-sovremennye-metody-setevoj-razvedki.38215/ (data zvernennya 02.06.2022).

5. Rozviduvalnyi protses za pohliadamy voiennykh fakhivtsiv NATO. URL: https://bintel.org.ua/nukma/rozviduvalnij-proces-nato/ (data zvernennia 02.06.2022).

6. Zhmur N.V. Mezhdunarodno-pravovye standarty zashhity informacii: otdelnye aspekty. *Legeasi Viata.* 2014. № 2/2 (266). S. 90-93.

Nataliia Zhmur, Mariia Zemlianikina

HISTORY OF FORMATION AND CURRENT STATE OF INFORMATION RETRIEVAL TECHNOLOGY OSINT

National Aviation University
Liubomyra Huzara Avenue, 1, 03680, Kyiv, Ukraine
E-mails: nataliia.zhmur@npp.nau.edu.ua, 5654340@stud.nau.edu.ua

Purpose: *defining the concept of OSINT as a technology for finding and using information from open sources, revealing the meaning, value, and essence of such a concept as «open source intelligence», as well as researching historical aspects and providing insights into the prospects of using OSINT technology.* ***Research methods:*** *documentary analysis and synthesis, comparative analysis, objective truth, cognitive-analytical, intersectoral method of legal research, historical, cognitive-analytical, etc.* ***Results:*** *addressing the historical stages of the formation of OSINT will provide an opportunity to improve the technology of search and use of information from open sources without violating the law.* ***Discussion:*** *based on the researched data the historical aspects of OSINT development and perspectives of the modern use of technology as one of the ways to obtain intelligence, NATO's experience in implementing technology in global intelligence, characterization, and analysis of intelligence value of open sources are analyzed.*

The role and value of intelligence technology from open sources of information «OSINT» is indisputable. Since the topic is not comprehensively researched, experts cannot come to a common opinion on the question: «What percentage of intelligence is obtained precisely from open sources of information?». Some estimate that 35 to 95 percent of the intelligence is collected, while the share of OSINT spending in the U.S. intelligence budget is about 1 percent. Another opinion is that the indicator is stable and equal to about 80%. This technique emerged relatively recently and has not yet been widely used in various countries of the world. But already quite a large number consider this concept powerful and perhaps one of the most promising means of intelligence for the future.

Key words: *intelligence; open sources of information; legality; information retrieval; cyberspace; analytics.*

Стаття надійшла до редакції 15.06.2022