УДК: 328.184: 355.404
DOI: https://doi.org/10.32689/2617-9660-2019-4(6)-201-208

Яровой Тихон Сергійович, *кандидат наук з державного управління, доцент, доцент кафедри публічного адміністрування, Міжрегіональна Академія управління персоналом, м. Київ. вул. Фрометівська, 2, тел.: 097-956-39-63, e-mail: tikhon_9563963@ukr.net*
ORCID: 0000-0002-7266-3829

OSINT, ЯК ПЕРСПЕКТИВНИЙ ІНСТРУМЕНТ КОНТРОЛЮ ЗА ЛОБІСТСЬКОЮ ДІЯЛЬНІСТЮ В КОНТЕКСТІ ДЕРЖАВНОЇ БЕЗПЕКИ

Анотація. Статтю присвячено дослідженню механізму отримання розвідувальної інформації з відкритих джерел (OSINT), як перспективного інструменту контролю за лобістською діяльністю в контексті державної безпеки.

Автором проаналізовано як вітчизняні так і зарубіжні підходи до розуміння процесу отримання розвідувальної інформації з відкритих джерел та запропоновано власне визначення OSINT. Окрему увагу присвячено класифікації джерел, які можуть бути використані у OSINT.

З огляду на те, що в Україні набуває дедалі більшої актуальності потреба регулювання лобізму, автором запропоновано створення Національної ради України з питань регулювання лобізму (НРУРЛ), як колегіального органу, орієнтованого на захист національних інтересів України та реалізацію державної безпеки.

У процесі дослідження визначено переваги OSINT для використання у процесі наглядової діяльності Національної ради України з питань регулювання лобізму. До таких віднесено: економію часу та ресурсів шляхом первинного збору інформації з відкритих джерел щодо діяльності суб'єктів лобіювання; можливість надання керівництву країни якісної аналітичної інформації про потенційно небезпечну діяльність суб'єктів лобіювання; можливість оприлюднення отриманої шляхом застосування OSINT інформації про порушення, здійснені суб'єктами лобіювання в процесі їх діяльності, з огляду на відкритий характер такої інформації (що дозволить відбивати інформаційні атаки недобросовісних лобістів та відкидати звинувачення у деспотії НРУРЛ). Додатково ефективність OSINT для НРУРЛ буде обумовлено тим, що до складу НРУРЛ входять фахівці з різних галузей знань та сфер діяльності.

На переконання автора, активне використання OSINT у діяльності НРУРЛ має стати запорукою ефективності регулювання лобізму в Україні, особливо у контексті державної безпеки.

Ключові слова: розвідка, відкриті джерела, інформація з відкритих джерел, збір розвідданих, OSINT, державна безпека, лобізм, Національна рада України з питань регулювання лобізму.

Yarovoi Tykhon Sergiyovych, *Candidate of Sciences (Public Administration), Associate Professor Interregional Academy of Personnel Management (Kyiv), Department of Public Administration, Ukraine. Interregional Academy of Personnel Management, 03039, Kyiv, Str. Frometivska, 2, tel.: 097-956-39-63, e-mail: tikhon_9563963@ukr.net*

ORCID: 0000-0002-7266-3829

OSINT AS A PROMISING TOOL FOR CONTROLLING LOBBYING ACTIVITIES IN THE CONTEXT OF NATIONAL SECURITY

Abstract. The article focuses on exploring the mechanism for obtaining open source intelligence (OSINT) as a promising tool for controlling lobbying activities in the context of national security.

The author analyzes both domestic and foreign approaches to understanding the process of obtaining intelligence from open sources and proposes his own definition of OSINT. Particular attention is given to classifying sources that can be used in OSINT.

Given the increasing need for lobbying in Ukraine, the author proposes the creation of a National Council of Ukraine on Lobbying Regulation (NCULR) as a collegial structur focused on protecting Ukraine's national interests and realizing national security.

The study identified the benefits of OSINT for use in the oversight activities of the National Council of Ukraine on lobbying regulation. These include: saving time and resources through the initial collection of open source information on the activities of lobbying entities; the ability to provide the country's leadership with high-quality analytical information on potentially dangerous activities of lobbying entities; the possibility of publicizing the information obtained through the use of OSINT regarding the illegal activities of lobbyists, given the open nature of such information (which will repel information attacks by unscrupulous lobbyists and dismiss for charges NCULR as a despot). Additionally, the effectiveness of OSINT for NURRL will be driven by the fact that NCULR is comprised of professionals from various fields of expertise and areas of activity.

According to the author, the active use of OSINT in NCULR activities should be the key to the effectiveness of lobbying regulation in Ukraine, especially in the context of state security.

Key words: intelligence, open source, open source information, intelligence collection, OSINT, state security, lobbying, National Council of Ukraine on Lobbying Regulation.

Постановка проблеми. Перехід українського суспільства у інформаційну епоху обумовив як зміну існуючих механізмів захисту національних інтересів та реалізації політики державної безпеки, так і запровадження нових механізмів, зокрема – підходів, форм, інструментів обробки великих масивів інформації як у цивільній, так і у військовій сферах.

Особливим інструментом роботи з інформації, який проявив себе у військовій розвідці, а згодом набув поширення у цивільній сфері, є діяльність по отриманню розвідувальної інформації з відкритих джерел (Open Source INTelligence, надалі – OSINT), що набу-

ває дедалі більшого значення, в тому числі – у процесі тотальної комп'ютеризації бізнесу, промисловості, державного управління, транспарентності всіх сфер життя у глобальній інформаційній мережі Інтернет.

Наразі, за результатами різних експертних оцінок, американські розвідувальні служби з відкритих джерел добувають від 35 % до 95 % розвіддаених. У провідних країнах світу система OSINT є важливим інструментом захисту національних інтересів та основною складовою в діяльності профільних силових відомств. Зокрема, в США та країнах НАТО існують окремі мережі центрів, що займаються збиранням та обробкою інформації з подальшим формуванням відповідних баз даних та практичним їх застосуванням для прийняття необхідних рішень. [1, с. 64]. В Україні, з 2014 року здійснюються окремі спроби використання OSINT у військовій діяльності, одначе використання цього інструменту у державному управлінні все ще перебуває на етапі наукових розробок, що й обумовлює актуальність теми нашого дослідження.

Аналіз останніх публікацій за проблематикою. Дослідженню проблематики контролю за лобістською діяльністю, в тому числі – в контексті забезпечення як національної безпеки в цілому, так і державної безпеки зокрема, присвячували свою увагу ряд вітчизняних вчених. Підґрунтям для даного дослідження стали окремі ідеї, напрацювання таких дослідників як О. В. Гросфельд, О. В. Дягілєв, Р. М. Мацкевич, І. П. Мігус, М. П. Недюха, В. Ф. Нестерович, А. М. Онупрієнко, О. Порфирович, В. В. Ровний, Є. О. Романенко, Г. П. Ситник, В. В. Сумська, Є. Б. Тихомирова, В. Л. Федоренко та інших. Окрім того, в роботі використано напрацювання щодо отримання розвідувальної інформації з відкритих джерел (OSINT) таких авторів як К. В. Власов, О. Ю. Іохов, О. В. Минько, В. Т. Оленченко, Н. Ф. Ржевська, та ряду інших.

Однак, дослідження перспективи використання OSINT для оцінки загроз державній безпеці у лобістській діяльності, досі лишаються по за увагою вітчизняної наукової спільноти, що ми й спробуємо надолужити.

Формулювання цілей (мети) статті. Дослідження механізму отримання розвідувальної інформації з відкритих джерел (OSINT), як перспективного інструменту контролю за лобістською діяльністю в контексті державної безпеки.

Виклад основного матеріалу дослідження. Для повноцінної аргументації доречності застосування розвідувальної інформації з відкритих джерел у процесі контролю за лобістською діяльністю та з огляду на відносну новизну такого інструменту розвідки як OSINT в українській науковій думці, в першу чергу вважаємо за доречне зупинитися на природі цього процесу.

На думку ряду вітчизняних дослідників отримання розвідувальної інформації з відкритих джерел (О. В. Минько, О. Ю. Іохов, В. Т. Оленченко, К. В. Власов), обмежується отриманням інформації з кіберпростору [2]. Ми не можемо погодитися з таким визначенням, як занадто звуженим. У вільному доступі перебуває величезна кількість джерел інформації, і обмежувати їх коло виключно кіберпростором – означає розглядати лише одну нішу OSINT.

Інші дослідники (Н.Ф. Ржевська, О. О. Кожушко), узагальнивши праці зарубіжних колег, вважають, що OSINT – одна з форм процесу організації та управління збором розвідувальних даних (Intelligence Collection Management), що включає їх пошук і відбір із публічних загальнодоступних джерел, добування та аналіз інформації, формування розвідувального документу для прийняття відповідного рішення [3, 4, 5]. Оскільки особливу увагу OSINT було присвячено в США, і зрештою, саме в США було вперше виокремлено цей інструмент розвідки, ми вважаємо, що доцільно також врахувати визначення, яке є унормованим в цій країні. Зокрема, відповідно до Закону США «National Defense Authorization Act for Fiscal Year 2006», розвідка відкритих джерел – це розвідка, що здійснюється шляхом збору, обробки та передачі цільовому адресату інформації з загально доступних відкритих джерел з метою вирішення конкретних завдань розвідки [6]. З огляду на це, вважаємо за доречне розглядати OSINT як таку форму роботи з розвідувальними даними, що включає їх пошук і відбір з публічних загальнодоступних джерел, подальшу класифікацію та аналіз інформації, з формуванням висновків, що надаються керівництву та можуть слугувати підставою для прийняття управлінських рішень.

В цілому, до джерел, що застосовуються в OSINT, відносять: у академічній сфері – 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; у державних, міждержавних та недержавних організаціях (NGOs) – бази даних, оприлюднена інформація, і друковані звіти, огляди широкого спектру в економіці, навколишньому середовищі, географії, гуманітарних науках, безпеки, науці і техніці; у комерційній та громадській сферах – 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; у індивідуальній і груповій сферах – рукописна, мальована, опублікована, друкована або поширена інформація (наприклад мистецтво, графіті, листівки, постери або веб-сайти) [7]. Тобто мова йде про вкрай широкий перелік джерел, який охоплює практично всі сфери діяльності людини.

Щодо пошуку інформації у відкритих джерелах, представлених в мережі Інтернет, то як зазначають з цього приводу згадувані вітчизняні дослідники OSINT, для цього використовуються різні пошукові системи. Це як універсальні пошукові системи, такі як Google, Yahoo, Ask, так і спеціалізовані (для пошуку мультимедійного контенту: фотографії, ілюстрації, малюнки, відео та аудіо файли тощо), такі як TinEye та Bing. Кожна з представлених пошукових систем має власні механізми та синтаксис запитів, що значно спрощує процес пошуку інформації, аналізу та відбору джерел [2, с. 81]. Таким чином, навіть для пошуку інформації в мережі Інтернет, потрібно мати певні ресурси, інакше

ефективність такого пошуку буде доволі низькою.

При цьому, в США існує і певна узагальнена класифікація відкритих джерел інформації. Їх розділяють на чотири основні категорії:

1. широко розповсюджені дані та інформація;
2. цільові комерційні дані;
3. експертні оцінки;
4. «сіра» література [8].

Доволі розмитий, на перший погляд, пункт «сіра література» має, тим не менш, доволі конкретне наповнення. Довідник НАТО (NATO Open Source Intelligence Reader) до «сірої літератури» відносить 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 [9]. Тобто мова йде про інформацію, яка не є таємною, але переважно використовується виключно фахівцями в тій чи іншій галузі і тому є важкодоступною або важкозрозумілою для нефахівця. Тобто ефективність застосування OSINT значною мірою залежатиме від наявності у складі структури, що збирає інформацію, фахівців різних галузей знань. Цей момент, в контексті нашого дослідження, є вкрай важливим.

У своїх попередніх дослідженнях автор неодноразово наполягав на потребі не лише легалізації лобіювання в Україні, але й створення відповідного регулятора – наглядового органу, здатного запобігти загрозам національній безпеці, які можуть стати наслідком безконтрольної лобістської діяльності. Зокрема, ключове місце в розробленому автором законопроекті посідає Національна рада України з питань регулювання лобізму (далі – НРУРЛ), яка є конституційним, постійно діючим колегіальним центральним органом виконавчої влади, що здійснює свою діяльність з метою забезпечення національної безпеки й інтересів України у процесі реєстрації та нагляду за лобістською діяльністю.

Відповідно до запропонованої концепції, Національна рада складається з двадцяти чотирьох осіб. З них сім членів НРУРЛ призначаються Верховною Радою України, сім членів НРУРЛ призначаються Президентом України, десять членів НРУРЛ є докторами наук (2 – доктори юридичних наук, 2 – доктори наук з державного управління, 2 – доктори економічних наук, 2 – доктори технічних наук, 2 – доктори медичних наук), яких обирає з'їзд представників вищих навчальних закладів та наукових установ, що є профільними у відповідних науках [10]. З урахуванням згадуваних нами вимог до ефективного OSINT, стає очевидним, що наявність у складі НРУРЛ науковців різних галузей знань сприятиме належному пошуку та аналізу інформації стосовно дій суб'єктів лобізму, які можуть нести загрозу національній безпеці у будь-якій сфері діяльності.

Доречність застосування OSINT у якості інструменту в контрольній та наглядовій діяльності НРУРЛ, обумовлена рядом специфічних переваг цього розвідувального методу. Для наглядності розуміння переваг застосування OSINT, звернемося до висловлювань американських та західноєвропейських фахівців. Відповідно

до даних зі згадуваного довідника НАТО по OSINT, застосування системи OSINT цінне тим, що дозволяє раціоналізувати інші розвідувальні ресурси, використавши їх на пошук лише тієї інформації, яка не може бути знайдена у відкритих джерелах [9]. Таким чином, застосування OSINT, як первинного інструменту контролю за діяльністю суб'єктів лобіювання, дозволить знизити витрати часу та ресурсів суб'єкту контролю, дозволяючи відсіювати несуттєві моменти, або ж навпаки – виявляти найбільш суперечливі, потенційно загрозливі для державної безпеки моменти в діяльності суб'єктів лобіювання уже на первинному етапі спостереження.

Також, на переконання військового керівництва США, розвідка відкритих джерел є значущим напрямом розвідувальної діяльності, який повинен бути інтегрований у розвідувальний цикл для гарантій того, що особи, які приймають рішення, формують політичний курс, цілком і повністю проінформовані [8]. У сфері контролю за лобістською діяльністю, активне застосування OSINT з боку НРУРЛ, дозволить не лише вчасно виявляти підстави для застосування тих чи інших санкцій до суб'єктів лобіювання, які порушують «правила гри», але й своєчасно інформувати Президента України, Прем'єр-Міністра України, інших посадових осіб, щодо спроб опосередкованого лобістського впливу на них та можливих наслідків цих спроб (наприклад, поширення суб'єктами лобіювання у ЗМІ матеріалів, спрямованих на активізацію протестних настроїв, з метою тиску на об'єкти лобіювання). Особливої ваги це набуває в контексті підтримання політичної стабільності в Україні, вжиття превентивних заходів, у тому числі – для забезпечення державної безпеки.

Окрім того, американські аналітики цінують OSINT за те, що розповсюдження та використання перевіреної інформації з відкритих джерел, дає змогу здійснювати обмін такою інформацією з зарубіжними союзниками, оскільки при її добуванні не використовуються приховані методи та секретні джерела [8]. Такий, здавалося б очевидний момент, означає, що регулятор лобістської діяльності (НРУРЛ), за потреби, може подавати інформацію, отриману з відкритих джерел, не лише до правоохоронних органів, з метою проведення розслідування та притягнення до відповідальності потенційних правопорушників, але і до засобів масової інформації. Це дозволить НРУРЛ значно послабити можливі (а з огляду на вітчизняні реалії, радше не просто можливі, а ймовірні, і дуже ймовірні) інформаційні атаки на себе з боку недобросовісних суб'єктів лобіювання, звинувачення в упередженості, обмеженні їх прав тощо. Адже, як відомо, транспарентність регулятора є одним з найбільш ефективних методів захисту його репутації від викривлення інформації та відвертої «демонізації» в очах громадськості.

Висновки і перспективи подальших досліджень. В процесі аналізу існуючих підходів до визначення OSINT, нами запропоновано власне визначення OSINT як такої форми роботи з розвідувальними даними, що включає їх пошук і відбір з публічних загальнодоступних джерел, подальшу класифікацію та аналіз інформації, з формуванням висновків, що надаються керівництву та можуть слугувати

підставою для прийняття управлінських рішень.

Доречність застосування OSINT у якості інструменту контрольної та наглядової діяльності НРУРЛ, обумовлена рядом специфічних переваг цього розвідувального методу.

По-перше, застосування OSINT, як первинного інструменту контролю за діяльністю суб'єктів лобіювання, дозволить знизити витрати часу та ресурсів суб'єкту контролю, дозволяючи відсіювати несуттєві моменти, або ж навпаки – виявляти найбільш суперечливі, потенційно загрозливі для державної безпеки моменти в діяльності суб'єктів лобіювання уже на первинному етапі спостереження.

По-друге, активне застосування OSINT з боку НРУРЛ, дозволить не лише вчасно виявляти підстави для застосування тих чи інших санкцій до суб'єктів лобіювання, які порушують «правила гри», але й своєчасно інформувати Президента України, Прем'єр-Міністра України, інших посадових осіб, щодо спроб опосередкованого лобістського впливу на них та можливих наслідків цих спроб.

По-третє, НРУРЛ, за потреби, може подавати інформацію, отриману з відкритих джерел, не лише до правоохоронних органів, з метою проведення розслідування та притягнення до відповідальності потенційних правопорушників, але і до засобів масової інформації. Це дозволить НРУРЛ значно послабити можливі інформаційні атаки на себе з боку недобросовісних суб'єктів лобіювання, звинувачення в упередженості, обмеженні їх прав тощо.

Наше дослідження, однак, не вичерпує всієї проблематики застосування OSINT з боку НРУРЛ. Більш детальне вивчення OSINT і перспектив його застосування органами державної влади, зокрема і в контексті забезпечення державної безпеки, ще чекає на своїх дослідників.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Пащенко Т. П. Гібридна війна та соціальні мережі. Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної науково-практичної конференції. Київ: НУОУ, 2017. С. 62-65.
2. Минько О. В. Використання технологій OSINT для отримання розвідувальної інформації / О. В. Минько, О. Ю. Іохов, В. Т. Оленченко, К. В. Власов // Системи управління, навігації та зв'язку. 2016. Вип. 4. С. 81-84.
3. Ржевська Н.Ф. Розвідка відкритих джерел (OPEN SOURCE INTELLIGENCE) Ржевська Н. Ф., Кожушко О. О. Розвідка відкритих джерел. URL: http://ena.lp.edu.ua/bitstream/ntb/19232/1/53-Rzhevska-257-261.pdf.
4. Доронин А. И. Бизнес-разведка / А.И. Доронин. 2-е изд., перераб. и доп. М., Ось-89, 2003. 384 с. URL: http://www.fb2book.com/?kniga=6313&strn=1&cht=1
5. Heather J. Williams, Ilana Blum. Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise https://www.rand.org/pubs/research_reports/RR1964.html
6. National defense authorization act for fiscal year 2006. URL: http://www.dod.gov/dodgc/olc/docs/PL109-163.pdf
7. Open source intelligence (Headquarters, Department of the Army) URL: https://fas.org/irp/doddir/army/fmi2-22-9.pdf
8. Open Source Intelligence (OSINT): Issues for Congress, December 5, 2007. URL: www.fas.org/sgp/crs/intel/RL34270.pdf

9. NATO Open Source Intelligence Handbook, November 2001. URL: http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf

10. Правове регулювання лобіювання в Україні: проблеми та перспективи: матеріали круглого столу (Київ, 24 квіт. 2019р.) / [ред..кол.: Мищак І. М., Тєлькінєна Т. Е., Яровой Т. С.] Київ, «Видавництьво Людмила». 2019. 104 с.

REFERENCES:

1. Pashchenko, T. P. (2017). Hibrydna viina ta sotsialni merezhi [Hybrid war and social networks]. *Informatsiinyi vymir hibrydnoi viiny: dosvid Ukrainy – Information dimension of hybrid warfare: Ukraine's experience:* Proceedings of international scientific practical conference. (pp. 62-65). Kyiv: NUOU [in Ukrainian].

2. Mynko, O. V., Iokhov, O. Yu., Olenchenko, V. T., Vlasov, K. V. (2016). Vykorystannia tekhnolohii OSINT dlia otrymannia rozviduvalnoi informatsii [Use of OSINT technologies for intelligence acquisition]. *Systemy upravlinnia, navihatsii ta zviazku – Control, navigation and communication systems, 4,* 81-84 [in Ukrainian].

3. Rzhevska, N. F., Kozhushko, O. O. (n.d.). Rozvidka vidkrytykh dzherel (OPEN SOURCE INTELLIGENCE) [Open Source Intelligence]. ena.lp.edu.ua. Retrieved from http://ena.lp.edu.ua/bitstream/ntb/19232/1/53-Rzhevska-257-261.pdf [in Ukrainian].

4. Doronin, A. I. (2003). *Biznes-razvedka [Business Intelligence].* (2nd ed.). Moscow: Os'-89 Retrieved from http://www.fb2book.com/?kniga=6313&strn=1&cht=1 [in Russian].

5. Williams, H. J., Blum, I. (n.d.). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. *www.rand.org.* Retrieved from https://www.rand.org/pubs/research_reports/RR1964.html [in English].

6. National defense authorization act for fiscal year 2006. (n.d.). *www.dod.gov.* Retrieved from http://www.dod.gov/dodgc/olc/docs/PL109-163.pdf [in English].

7. Open source intelligence (Headquarters, Department of the Army). (2006). *fas.org.* Retrieved from https://fas.org/irp/doddir/army/fmi2-22-9.pdf [in English].

8. Open Source Intelligence (OSINT): Issues for Congress, December 5, 2007. (n.d.). *fas.org.* Retrieved from www.fas.org/sgp/crs/intel/RL34270.pdf [in English].

9. NATO Open Source Intelligence Handbook. (2001). *www.oss.net.* Retrieved from http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf [in English].

10. Myshchak, I. M., Tielkiniena, T. E., Yarovoi, T. S. (Eds.). (2019). *Pravove rehuliuvannia lobiiuvannia v Ukraini: problemy ta perspektyvy: materialy kruhloho stolu – Legal Regulation of Lobbying in Ukraine: Problems and Prospects:* Proceedings of Round Table. Kyiv, «Vydavnytsvo Liudmyla» [in Ukrainian].