2. Кибербезопасность: на что глобальные компании потратят $76,9 млрд. IT GROUP DF, 2014. http://www. delo.ua
3. Word Politics, Security and International Law in Cyber Space. Australian Centre for Cyber Security. UNSW, Canberra. http://www.unsw.adfa.edu.au
4. Convention on Cybercrime. Budapest, 23/11/2001. https://www.coe.int

Ключові слова: кібербезпека, глобальні загрози у світі, захист системи кібербезпеки, надійність системи кіберпростору.
Key words: cybersecurity, global threats in the world, protection of cybersecurity system, reliability of cyberspace system.

УФІМЦЕВА ОЛЕНА СЕРГІЇВНА

Національна академія Служби безпеки України,
провідний науковий співробітник, кандидат юридичних наук

ВИКОРИСТАННЯ OSINT В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ РФ ПРОТИ УКРАЇНИ

Однією зі складових збройної агресії РФ проти України є інформаційна війна, метою якої є послабити моральний дух українців і їхню віру в перемогу, для чого використовуються різноманітні фейки та пропагандистські матеріали. З початком російської агресії щодо України питання отримання інформації з відкритих джерел і розвінчання фейків отримало нове звучання [1].

Протидія інформаційним впливам включає з-поміж іншого формування умінь та навичок працювати з інформацією он-лайн, перевіряти її, а також використання методів критичного аналізу для спростування викладеної інформації.

В умовах глобалізації, цифровізації, стрімкого розвитку інформаційних технологій існує безліч джерел і масивів інформації, достовірність якої потребує обов'язкової перевірки. За кількістю інформації саме мережа Інтернет знаходиться на першому місці у світі, випереджаючи ЗМІ, галузеві видання і одержувані від колег новини, спеціальні огляди, закриті бази даних [1]. Проте найбільшою проблемою є знаходження загальнодоступних змістовних і надійних джерел. У таких умовах надзвичайно важливим інструментом стає OSINT, який передбачає пошук інформації з відкритих, тобто загальнодоступних, джерел, її збір, співставлення та аналіз.

OSINT – термін який розшифровується як open-source intelligence, – це методи пошуку, збору, вибору та аналізу інформації, яка являє оперативний інтерес, з відкритих джерел. Отримані таким чином дані використовують маркетологи, журналісти, фахівці з комп'ютерної та інтернет-безпеки та ін. [1]. Вперше термін OSINT був використаний військовими і розвідувальними службами для позначення збору стратегічно важли-

вої, але загальнодоступної інформації з питань національної безпеки [2]. За результатами різних експертних оцінок, американські розвідувальні служби з відкритих джерел добувають від 35 % до 95 % розвідданих [3].

Один із прикладів верифікації за допомогою OSINT інформації, яка з'являється в мережі Інтернет, мітиться у публікації міжнародної волонтерської спільноти InformNapalm і демонструє, яким чином можна перевірити, відповідає чи ні дійсності статистика втрат ЗС РФ станом на 24.03.2022 [4].

Міністерство оборони РФ вперше офіційно відзвітувало про втрати серед своїх військових 02.02.2022 – за його даними станом на цей день було вбито 498 і поранено 1597 осіб. Аналіз повідомлень з російських ЗМІ і соціальних мереж свідчить про нагородження російських військових, які брали участь у війні з Україною, при чому це відбувалося здебільшого посмертно. Судячи з цих повідомлень, загиблі отримували Орден Мужності. Більшість військовослужбовців були нагороджені указом президента РФ від 03.03.2022. Мінімальний номер «посмертного» Ордену Мужності – 78487, максимальний – 83281. Різниця між ними становить 4794 ордени. Тобто можна стверджувати, що саме це – мінімальна кількість загиблих військовослужбовців ЗС РФ [4].

Технології і методики OSINT дозволяють отримати якнайбільше потрібної інформації у короткий термін та витрачаючи щонайменше ресурсів (існує достатня кількість безкоштовних інструментів OSINT), що є досить важливим в умовах воєнного стану. Зауважимо, що близько 40 % всієї інформації в Інтернеті є безкоштовною [1].

Особливістю OSINT можна назвати те, що це завжди специфічна інформація, зібрана й структурована особливим чином для відповіді на конкретні запитання [5]. До її переваг можна віднести доступність різноманітних джерел інформації, а також обсяг її масивів, різносторонність інформації, велику кількість існуючих технік, методик і технологій. Кінцевим результатом OSINT завжди є певні знання, отримані у результаті висновків з отриманої інформації. За допомогою OSINT у сьогочасному світі вирішуються абсолютно різноманітні завдання на рівні держави, як то забезпечення національної безпеки або боротьба з тероризмом. Інструменти та технології OSINT дозволяють відстежувати погляди громадськості на різні теми, висвітлення з різних боків подій, що відбуваються у світі, отримувати потрібну інформацію для прийняття управлінських рішень.

У провідних країнах світу OSINT є одним із важливих інструментів захисту національних інтересів, а також основною складовою в діяльності профільних силових відомств. Так, у 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 [6].

Таким чином, можна стверджувати, що стрімке зростання цінності та ролі інформації, розвиток інформаційних технологій, а також досту-

пність мережі Інтернет та збільшення масиву загальнодоступної інформації робить пошук, збір, співвідношення, відбір та аналіз інформації з відкритих джерел (таких як ЗМІ, соціальні мережі, форуми та блоги, державні дані, публікації чи комерційні дані) одним із дієвих сучасних засобів протидії інформаційній війні в умовах збройної агресії РФ проти нашої держави.

Список використаних джерел:

1. Ланде Д. В. Правові питання конкурентної розвідки // Інформація і право. 2020. № 2(33). URL: http://ippi.org.ua/lande-dv-pravovi-pitannya-konkurentnoi-rozvidki-st-51-68 (дата звернення: 21.05.2022).
2. Исследование на основе открытых источников или OSINT: где используется и в чем опасность. URL: https://eset.ua/ru/blog/view/117/issledovaniye-na-osnove-otkrytykh-istochnikov-ili-osint-gde-ispolzuyetsya-i-v-chem-opasnost (дата звернення: 21.05.2022).
3. Яровой Т. С. OSINT, як перспективний інструмент контролю за лобістською діяльністю в контексті державної безпеки. URL: https://maup.com.ua/assets/files/expert/6/18.pdf (дата звернення: 21.05.2022).
4. «Медальний залік»: OSINT аналіз справжніх втрат РФ за перший тиждень бойових дій в Україні. URL: https://informnapalm.org/ua/medalnyi-zalik-analiz-osint/ (дата звернення: 21.05.2022).
5. Щурат Т. Г., Смук А. О. Деякі аспекти розвідки з відкритих джерел інформації (OSINT). URL: http://dspace.oduvs.edu.ua/bitstream/123456789/654/1/6.pdf (дата звернення: 21.05.2022).
6. 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.

Ключові слова: розвідка з відкритих джерел, інформаційна війна, збирання інформації, збройна агресія.

Key words: open-source intelligence, information war, gathering information, armed aggression.

БАЛАНДІНА НАТАЛІЯ МИКОЛАЇВНА

Національний університет «Одеська юридична академія», старший викладач кафедри кібербезпеки

РОЛЬ МАТЕМАТИЧНОЇ КУЛЬТУРИ У СУЧАСНОМУ ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Сучасні трансформаційні процеси цивілізаційного розвитку зумовлюють постійне звернення держав світу до якості людського життя і проникнення цих тенденцій до усіх сфер буття людини. Вказана інтеграція не оминає і освітню сферу, яка є стратегічним ресурсом