

Данилевський А. О.,
начальник кафедри розвідки – начальник розвідки,
кандидат юридичних наук, доцент
Данилівський Л. Й.,
старший викладач кафедри розвідки
(Київський інститут Національної гвардії України)

РОЛЬ OSINT В СИСТЕМІ РОЗВІДУВАЛЬНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

У сучасному світі Інтернет та обмін інформацією настільки увійшли в повсякденне життя людини, що практично не залишають місця для анонімності. Практично будь-яка людина так чи інакше залишає певні цифрові сліди в кіберпросторі, що дає можливість аналітикам OSINT виявляти таку інформацію про людей завдяки легкому доступу до величезної кількості інформації, дозволяючи деанонімізувати осіб в інтернет-просторі [1, с. 20]. Проте така інформація може бути використана як для захисту державної безпеки, так і у протиправних цілях. Доступність інформації та інструментів її обробки дозволяють використовувати методи OSINT різним прошаркам населення. Саме тому правоохоронні органи повинні приділяти цьому напрямку пильну увагу, щоб не опинитися у статусі «наздоганяючих» та не програти технологічні перегони криміналітету та ворогу.

Питання методів OSINT розглядали у своїх роботах О. В. Ангельська, В. В. Бурба, А. Л. Главацька, К. Ю. Ісмайлов, І. Р. Опірський, М. І. Пашковський, А. О. Смук, О. С. Уфімцева, Т. Г. Щурат, Т. С. Яровой та інші дослідники. Проте в їх роботах недостатньо уваги приділяється дослідженню використання методів OSINT у правоохоронній діяльності, зокрема діяльності Національної гвардії України.

Метою цієї роботи є аналіз ролі OSINT в системі розвідувального забезпечення діяльності Національної гвардії України.

OSINT – термін який розшифровується як open-source intelligence, – це методи пошуку, збору, вибору та аналізу інформації, яка являє оперативний інтерес (розвідка), з відкритих джерел. Вперше термін OSINT був використаний військовими і розвідувальними службами для позначення збору стратегічно важливої, але загальнодоступної інформації з питань національної безпеки. За результатами різних експертних оцінок, американські розвідувальні служби з відкритих джерел добувають від 35 % до 95 % розвідданих [2, с. 762].

Збирання інформації з відкритих джерел може здійснюватися вручну за стандартизованою процедурою або бути автоматизованим за допомогою різноманітних інструментів або сценаріїв. В останньому випадку ланцюг забезпечення збереження може створюватися також автоматично (програмно). Особливо актуальним є використання програмних інструментів або сценаріїв в процесі відшукування належної інформації, наприклад для вебскрапінгу (від англ. scraping) – перетворення у структуровані дані інформації з вебсторінок [3, с. 85].

Розвідка з відкритих джерел відрізняється від інших видів розвідки в першу чергу специфічною категорією технічних і людських ресурсів, джерелами отримання інформації та методами її збору. На відміну від таємної інформації, перевірену інформацію з відкритих джерел можливо розповсюджувати та використовувати без застосування відповідних грифів, що дає змогу обмінюватися такою інформацією, оскільки при її добуванні не використовуються приховані методи та секретні джерела. Проте слід погодитися з дослідниками, які зазначають, що це не розповсюджується на аналітичну довідку з такої інформації [4, с. 112].

Дослідження досвіду європейських країн показує, 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 [5, с. 18].

Як вже зазначалося, характерною особливістю OSINT є те, що його методи є доступними для використання будь-якою особою, це не розвідка в класичному розумінні, визначена положеннями Закону України «Про розвідку», а отже, відносно OSINT не діє заборона, закріплена у частині 2 статті 5 зазначеного закону, щодо заборони здійснення розвідувальної діяльності суб'єктами, які не відносяться до розвідувальних органів відповідно до закону. Це надзвичайно актуально для Національної гвардії України, яка на сьогоднішній день не входить ані до кола розвідувальних органів, ані до розвідувального товариства. Таким чином використання методів OSINT в діяльності Національної гвардії України не суперечить чинному законодавству.

Розглядаючи OSINT крізь призму завдань Національної гвардії України, визначених Законом України «Про Національну гвардію України», можна виділити наступні сфери використання OSINT:

1) Кримінальна розвідка – комплекс заходів, спрямованих на своєчасне запобігання, виявлення і нейтралізацію реальних та потенційних загроз національним інтересам України від протиправних посягань [5, с. 111]. Завдяки використанню OSINT підрозділи Національної гвардії України можуть отримувати інформацію щодо можливих загроз терористичної діяльності, організованої злочинності та інших протиправних посягань під час виконання завдань з охорони громадської безпеки та порядку, проведення масових заходів, охорони важливих державних об'єктів, охорони спеціальних вантажів тощо. Наприклад, моніторинг соціальних мереж та профільних груп чи форумів дозволяє оцінити приблизну кількість учасників масового заходу, наявність серед них радикально налаштованих елементів та потенційних провокаторів.

2) Військова розвідка – найважливіший вид бойового забезпечення, що полягає у добуванні, зборі та узагальненні відомостей про противника, характер його дій і наміри, сильних та слабкі сторони, а також ступінь та характер інженерного обладнання займаних ним районів та позицій, системи загороджень, нові засоби боротьби та способи дій в бою. Завдяки використанню OSINT підрозділи Національної гвардії України можуть отримувати інформацію про противника, виявлення його позицій, переміщення сил, логістичних маршрутів тощо. Аналіз супутникових знімків, перехоплення незашифрованих повідомлень, аналіз соціальних мереж російських військових можуть дати цінну інформацію про противника. Аналіз фото- та відеоматеріалів дозволяє оцінити приблизні втрати техніки та особового складу. Так, дослідники відзначають, що OSINT дозволяє:

- виявляти рух ворожих військ. Збір інформації про рух ворожих військ, їхню кількість та розташування допомагає військовим командирам приймати обґрунтовані рішення та своєчасно реагувати на загрози;

- аналізувати тактику і стратегію ворога. OSINT допомагає виявити тактику та стратегію ворога, що дає можливість українським військовим адаптувати свої дії для ефективного протистояння;

- збирати інформації про зброю і техніку. Аналіз відкритих джерел дозволяє виявляти та відстежувати рух військової техніки та зброї ворога, а також визначати нові типи зброї, які вони можуть використовувати [1, с. 41-42].

3) Протидія дезінформації та ворожого ІІСО.

Таким чином, можна зробити висновок, що OSINT займає важливе місце у системі розвідувального забезпечення діяльності підрозділів Національної гвардії України. У поєднанні з іншими видами розвідки розвідка з відкритих джерел здатна значно підвищити ефективність діяльності підрозділів Національної гвардії України та результативність прийняття рішення командирами, що підтверджується досвідом правоохоронних органів європейських країн.

Водночас, незважаючи на доступність, ефективне використання OSINT вимагає специфічних знань і навичок, таких як знання технік пошуку, методології аналізу даних та розуміння юридичних аспектів, пов'язаних із використанням відкритої інформації. Крім того, у контексті сучасних загроз, таких як дезінформація та фейкові новини, критичне мислення та вміння відрізнити надійні джерела стають важливими елементами OSINT-досліджень [6, с. 3]. Тому, на нашу думку, для ефективного використання OSINT при виконанні службово-бойових завдань необхідно включати дослідження методів OSINT в систему підготовки майбутніх офіцерів Національної гвардії України.

1. Главацька А. Л., Ангельська О. В., Опірський І. Р. Дослідження технології використання OSINT як нової загрози з деанонізації особи в інтернет просторі. *Кібербезпека: освіта, наука, техніка*. 2024. № 1. С. 19-50.

2. Уфімцева О. С. Використання OSINT в умовах збройної агресії РФ проти України. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.)*. Одеса : Видавничий дім «Гельветика», 2022. Т. 1. С. 761-763.

3. Пашковський М. І. Особливості використання OSINT при документуванні та розслідуванні колабораційної діяльності. *Актуальні питання кримінально-правової кваліфікації, документування та розслідування колабораціонізму : матеріали Всеукр. науково-практ. конф., м. Одеса, 21 лип. 2022 р.* Одеса, 2022. С. 82–86.

4. Ісмаїлов К. Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації. *Південноукраїнський правничий часопис*. 2016. № 2. С. 110-113.

5. Бурба В. В. Організаційно-правові засади використання розвідки з відкритих джерел інформації (OSINT) в діяльності розвідувальних служб європейських країн. *Юридичний бюлетень*. 2019. Вип. 11. Ч. 1. С. 11-19.

6. Думчиков М. О. Використання OSINT технологій для виявлення корупційних правопорушень: сучасні підходи та виклики. *Академічні візії*. 2024. Вип. 36. С. 1-6.