УДК 355.4

О.В. Минько, О. Ю. Іохов, В.Т. Оленченко, К.В. Власов

Національна академія Національної гвардії України, Харків

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ OSINT ДЛЯ ОТРИМАННЯ РОЗВІДУВАЛЬНОЇ ІНФОРМАЦІЇ

Розкрито сутність діяльності з отримання розвідувальної інформації з відкритих джерел - OSINT (Open Source INTelligence) та визначені перспективи використання сучасних розвідувальних технологій у Національній гвардії України.

Ключові слова: *інформаційний простір, розвідка, технології.*

Вступ

Постановка проблеми. Сучасне людство є свідком динамічних глобальних світових змін, стрімкого переходу від індустріального суспільства до інформаційного. Такі об'єктивні зміни вимагають оновлення форм, умов та способів праці у всіх, без виключення, спектрах діяльності людини, від легкого виробництва та аграрної промисловості до програмно-комп'ютерного забезпечення і космічних досліджень всесвіту.

Змінюються умови та фактори збройної боротьби, виникають інноваційні способи застосування збройних сил.

В арміях провідних країн світу виникають нові способи добування розвідувальної інформації, інформаційної підтримки управлінських процесів та рішень. Динамічний інформаційний розвиток сучасного суспільства створив об'єктивні чинники для виникнення умов, коли все більше інформації, яка необхідна для прийняття рішення, можливо знайти у відкритих джерелах кіберпростору (Інтернету).

Діяльність по отриманню розвідувальної інформації з відкритих джерел кіберпростору отримала назву OSINT – Open Source INTelligence (відкриті джерела розвідки).

16 травня 2011 року уряд Сполучених Штатів Америки прийняв Міжнародну стратегію діяльності США у кіберпросторі (U.S. International Strategy for Cyberspace). За різними оцінками, з відкритих джерел кіберпростору американські розвідувальні служби добувають від 35% до 95% розвідувальної інформації. При цьому доля витрат на розвідку відкритих джерел в розвідувальному бюджеті США складає приблизно 1%[1].

На фоні стрімкого розвитку сучасних інформаційних технологій даному виду розвідки приділяється все більше уваги і у відповідних силових структурах України. Нажаль, у Національній гвардії України поки що не надається істотного значення використанню методів OSINT для отримання розвідувальної інформації та її аналізу. Можливо це пов'язано, з дещо архаїчними поглядами на саме поняття інформаційного суспільства, коли спрацьовує принцип «простіше заборонити (нічого не робити), ніж розглянути нові можливості». Зазвичай, як і раніше, використовуються старі інструкції при використанні матеріалів з мережі Інтернет, а з початком проведення АТО – і нові заборони з використання певних інформаційних ресурсів.

Мета статті – дати уявлення про перспективи використання технології OSINT, як одного із способів отримання розвідувальної інформації у процесі службово-бойової діяльності Національної гвардії України.

Виклад основного матеріалу

Розвідка на основі аналізу відкритих джерел інформації далеко не новий вид діяльності для розвідувальних органів провідних країн світу і зі стрімким розвитком інформаційних технологій методи її використання мають бути об'єктом відповідних досліджень.

Збір розвідувальної інформації в OSINT суттєво відрізняється від інших напрямів розвідувальної діяльності, насамперед агентурної розвідки. При роботі з агентурними методами головна проблема полягає у добуванні інформації з джерела, що не завжди схильне до співпраці. В OSINT головним питанням є пошук змістовних та надійних джерел серед величезної кількості різноманітної інформації кіберпростору.

Для пошуку інформації у відкритих джерелах, представлених в мережі Інтернет, використовуються різні пошукові системи. Це універсальні пошукові системи, такі як Google, Yandex, Yahoo, Ask та 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. Слід зазначити, що наведена методика роботи за принципами OSINT вже активно використовується у бізнес-колах провідних країн світу для пошуку та отримання законними шляхами інформації про партнерів та конкурентів [1].

Одним із різновидів інформаційних технологій збору та аналізу інформації з відкритих джерел є ще один напрямок розвідки – HUMINT (human intelligence), у дослівному перекладі - «розвідка по людям».

Якщо раніше під терміном HUMINT розуміли збір розвідувальної інформації за допомогою різного роду шпигунів та агентів, то в теперішній час під терміном HUMINT також розуміють діяльність та заходи, що спрямовані на збір інформації з використанням оперативної психології. До таких технологій відносяться: моніторинг соціальних мереж, опитування, соціальний інженірінг, залегендовані бесіди (під виглядом журналіста, клієнта, роботодавця і т.п.).

У сучасному світі технології OSINT та HUMINT значно пов’язані між собою і використовують значну кількість технологічно подібних методів отримання необхідної інформації про об’єкт розвідки.

Закордонний досвід. OSINT не новий вид діяльності для американської розвідки. Це одна з семи розвідувальних дисциплін (так в розвідтоваристві називають види розвідки в залежності від типу залучених сил або коштів), яка застосовується ще з часів Другої світової війни.

Розвідку на основі аналізу відкритих джерел інформації використовують в розвідувальному співтоваристві США з лютого 1941 року, тобто з моменту формування у складі комісії з комунікацій Інформаційної служби зарубіжного мовлення (Foreign Broadcast Information Service – FBIS).

Для створення служби, головним завданням якої став контроль радіомовлення країн нацистського блоку, президент Рузвельт виділив 150 000 дол. (у той час на ці гроші можна було побудувати чотири літака Р-51 «Мустанг», що стали згодом кращими винищувачами ВПС США Другої світової). Вже у листопаді 1941 року у Портланді, штат Орегон, була розгорнута і перша станція моніторингу.

З початком війни FBIS передали до складу міністерства оборони, а після її закінчення – в ЦРУ. За однією з легенд класичним прикладом діяльності служби під час Другої світової війни стало визначення ефективності нанесення авіа ударів військами сил антигітлерівської коаліції по залізничних мостах в залежності від коливань цін на апельсини в Парижі.

2004 рік ознаменувався для американської розвідки початком нового етапу масштабного реформування. В цьому році Джордж Буш підписав закон «Про реформування розвідки та протидії терористичній загрозі», що містить вказівки про включення OSINT-розвідки в якості повноцінної і рівноправної розвідувальної дисципліни в діяльність американської розвідки, а також про формування Національного центру розвідки на основі аналізу відкритих джерел інформації.

Сьогодні фахівці нового центру щодня готують більше 2000 документів, включаючи перекази, аналітичні огляди, відеопідбірки, карти та ін. Тематика документів охоплює практично всі важливі сфери: міжнародну політику; військову, економічну, наукову і технологічну сфери; боротьбу з тероризмом; контроль за розповсюдженням військових технологій; внутрішню безпеку і так далі.

Більш того, зараз у США сформована розгалужена мережа центрів і пунктів, які ведуть розвідку на основі аналізу відкритих джерел інформації і надають відомості більш ніж 7000 споживачам розвідданих.

І це не що інше, як результат скоординованих дій законодавчої та виконавчої влади, спрямованих на здійснення цілеспрямованої політики в галузі забезпечення національної безпеки.

Окремої уваги заслуговує розвідка на основі аналізу відкритих джерел інформації у військовому відомстві США. Пояснюється це не тільки особливим інтересом до подібної розвід-дисципліни з боку Пентагону, але і тим, що така розвідка стала невід'ємною частиною будь-якої розвідувальної операції ЗС США.

Більше того, американські аналітики відзначають, що прямо або побічно зібрана таким чином інформація стає базою для всіх подібних операцій і розроблюваних документів, а її доступність дозволяє розвідслужбам вирішувати широке коло завдань без залучення фахівців агентурної розвідки і застосування технічних засобів збору інформації. Дані, отримані в ході цього виду розвідки, справляють істотний вплив на організацію будівництва збройних сил, забезпечення їх готовності, а також на ефективне планування бойових дій.

Сьогодні всі центри OSINT-розвідки у складі відомств розвідувального співтовариства об'єднані в єдину інформаційну систему, що отримала назву як інформаційна система відкритих джерел інформації (OSIS)[1].

Досвід України. Технології OSINT активно використовуються в ході російсько–української війни в окремих районах Донецької та Луганської областей. Наприклад, одним із джерел інформації про результативність артилерійських обстрілів вогневих позицій терористами у районі Донецька є обговорення даних подій мешканцями міста в мережі, а фотографії військової техніки, зроблені місцевими жителями, часом значно ефективніші за результати моніторингу представниками ОБСЄ.

В мережі Інтернет існує безліч ресурсів, що дозволяють розвідувальним органам отримувати інформацію про незаконні збройні формування у зоні проведення АТО. Наприклад, на основі даних OSINT-розвідки, яку проводять волонтери команди InformNapalm, визначаючи за геотегами та записами у соціальних мережах місце розташування російських солдатів, була створена «таблиця шевронів» підрозділів ЗС РФ, що «засвітилися» у конфлікті на Донбасі. Фактично, це стало одним з інструментів ідентифікації підрозділів і частин РФ, що воюють проти України на Донбасі.

В Україні таких організацій та ресурсів, що ведуть пошук інформації або здійснюють протидію ворожій пропаганді, на даний час вже налічується десятки. Наприклад, деякі з них:

- Dokaz - ресурс, який публікує докази присутності російських військових на сході України, матеріали щодо злочинів терористів та окупантів на території українського Донбасу [2].
- Bellingcat Ukraine Conflict Vehicle Tracking Project - на цьому сайті збираються та публікуються дані щодо пересування російської військової техніки на Донбасі [3].
- Стоптеррор - проект візуалізує на інтерактивній карті бойові дії на території України, публікується інформація про незаконні збройні формування і присутність кадрових військових РФ [4]. Також через сайт можна повідомляти про будь-які інші події за темою сайту.

Вже зараз деякі ресурси, що використовують технології OSINT, і які є доступними у мережі Інтернет, використовуються військовослужбовцями у зоні проведення АТО, у тому числі і військовослужбовцями НГУ, що несуть службу на блокпостах, проводять оперативно-профілактичні відпрацювання, пошукові та інші спеціальні заходи.

Досить часто використовуються можливості сайту «Миротворець» [5]. Даний сайт розроблений Центром «Миротворець», який є незалежною недержавною організацією , створеною групою вчених, журналістів і фахівців з питань дослідження ознак злочинів проти національної безпеки України, світу, безпеки людства та міжнародного правопорядку, що займаються творчою наукової та журналістською діяльністю.

Центр «Миротворець» здійснює свою діяльність у суворій відповідності до чинного законодавства України та міжнародними нормативно-правовими актами, ратифікованими нашою державою.

Інформаційне наповнення сайту «Миротворець» здійснюється із загальновідомих і загальнодоступних відкритих джерел, які використовуються виключно в науково-дослідних, творчих і журналістських цілях.

Основними джерелами інформації, що використовується Центром «Миротворець» для проведення своїх досліджень, є відкриті для загального доступу матеріали, які друкуються і розміщуються в соціальних мережах, web-виданнях, на приватних web-сторінках, в спеціалізованих форумах і блогах, транслюються по каналам телебачення і радіомовлення.

Окрім інформації про окремих осіб, на сайті створена карта військових частин, підрозділи яких брали і беруть участь у війні проти України.

На даний час Центр «Миротворець» не заперечує проти використання інформації і відомостей, що містяться на однойменному сайті, співробітниками СБУ, МВС України, Державної прикордонної служби України, ЗС України та Національної гвардії України в оперативній і розшукової діяльності.

Такий сайт та інші подібні до нього Web-ресурси значно полегшують роботу працівників правоохоронних органів держави.

Крім того, завдяки тому, що бойовики розміщують свої дані та фото в соціальних мережах, усі небайдужі бажаючі можуть долучатись до збору розвідувальних даних про противника.

Яскравий приклад – це інформація зібрана про громадянина РФ Олексія Мільчакова, садиста-нациста, що воював проти українських Збройних Сил у ході конфлікту на Донбасі та про скоєні ним злочини.

Використання сучасних технологій значно спрощує розкриття складу сил протиборчої сторони.

Вже зараз елементи OSINT активно використовуються Службою Безпеки України, Головним Управлінням Розвідки, Міністерством внутрішніх справ.

Також досить часто інформація, отримана за допомогою OSINT використовується в ході інформаційної війни проти противника.

Разом з тим, не слід забувати, що подібні методи пошуку розвідувальних даних активно використовує і противник, що потребує самодисципліні-

ни особового складу Національної гвардії України щодо розміщення відомостей в соціальних мережах, які можуть становити інтерес розвідки противника, на що неодноразово звертало увагу Головне Управління НГУ.

Висновки

Розвиток комп'ютерних технологій та доступність Інтернету і, відповідно, збільшення потоку відкритої інформації робить актуальним проблему аналізу її джерел як одного із елементів сучасної системи управління.

Застосовувана сьогодні в провідних країнах світу сукупність сучасних технологій дозволяє співробітникам розвідки отримувати доступ до великих масивів даних, необхідних для оцінювання ситуації, здійснення контролю за обстановкою та задоволення потреб органів управління в даних, необхідних для прийняття обгрунтованих і правильних рішень.

З урахуванням останніх подій, виглядає доцільним створення в Україні підрозділів, що займалися б попередньою обробкою і аналізом інформаційних потоків, у тому числі і OSINT-розвідкою. Можна відмітити спроби Міністерства інформаційної політики України реалізувати подібні проекти, однак на даний момент перевага на боці волонтерських недержавних організацій, що розуміють важливість використання технологій в процесі інформаційної боротьби і пропонують свої послуги збройним формуванням України.

Досвід провідних країн світу у галузі аналізу відкритих джерел інформації для потреб розвідки дозволяє визначити перспективні напрямки для Національної гвардії України:

1) створення відділів (груп) аналізу відкритих джерел інформації, які б працювали у взаємодії з подібними органами МВС, ЗС та інших силових структур України;

2) активне використання можливостей сучасних інформаційних технологій у процесі отримання, оброблення та аналізу інформації для потреб як розвідки, так і органів управління;

3) створення спеціального захищеного Web-порталу, що має містити чати, дошки повідомлень, адреси і телефони подібних органів інших формувань та структур, призначених для обміну даними аналізу.

Існує необхідність використання технологій OSINT Національною гвардією України не тільки в зоні проведення АТО, але і під час моніторингу суспільно-політичної обстановки в Державі з метою запобігання або у ході можливих масових порушень громадського порядку, актів громадянської непокори, протестів та терористичних актів, а також у процесі прийняття управлінських рішень і планування операцій (бойових дій).

Список літератури

1. Разведка из открытых источников [Електронний ресурс]. Режим доступу: http://z-filez.info/story/razvedka-iz-otkrytykh-istochnikov.

2. Dokaz. [Електронний ресурс]. Режим доступу: http://www.dokaz.org.ua/ - Назва з екрану.

3. Bellingcat Ukraine Conflict Vehicle Tracking Project [Електронний ресурс]. Режим доступу: https://www.bellingcat.com/resources/2015/02/12/ukraine-conflict-vehicle-first-week/ - Назва з екрану.

4. Стоптеррор [Електронний ресурс]. Режим доступу: http://stop-terror.com.ua/- Назва з екрану.

5. Центр «Миротворець» [Електронний ресурс]. Режим доступу: https://myrotvorets.center/- Назва з екрану.

Надано до редакції 15.10.2016

Рецензент: д-р тех. наук, проф. О.О. Морозов, Національна академія Національної гвардії України, Харків.

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ OSINT ДЛЯ ПОЛУЧЕНИЯ РАЗВЕДЫВАТЕЛЬНОЙ ИНФОРМАЦИИ

А.В. Минько, А.Ю. Иохов, В.Т. Оленченко, К.В. Власов

Раскрыта суть деятельности по получению разведывательной информации из открытых источников - OSINT (Open Source INTelligence) и определены перспективы использования современных разведывательных технологий в Национальной гвардии Украины.

Ключевые слова: *информационное пространство, разведка, технологии.*

USING OF OSINT TECNOLOGIES FOR INTELLIGENCE

O.V. Mynko, A.Yu. Iohov, V.T. Olenchenko, K.V. Vlasov

The essence of intelligence to obtain information from public sources - OSINT (Open Source INTelligence) and identified prospects of using modern exploration technologies in the National Guard of Ukraine.

Keywords: *information space, intelligence, technologies.*