УДК 327(045)

Андрій Володимирович СЕРВАТОВСЬКИЙ,
слухач магістратури факультету № 1 (слідства)
Харківського національного університету внутрішніх справ;
Юрій Миколайович ОНИЩЕНКО,
кандидат наук з державного управління, доцент,
доцент кафедри кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-7755-3071;
Павло Валентинович МАКАРЕНКО,
кандидат психологічних наук, доцент,
заступник декана з навчально-методичної роботи
факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-9055-3287

МІЖНАРОДНИЙ ДОСВІД ВИКОРИСТАННЯ OSINT

На сьогоднішній день немає такої людини яка б не користувалася соціальними мережами, багато злочинів які відбуваються у сучасному світі плануються саме в інтернет-просторі, через спілкування в месенджерах, надсилання фото з зашифрованим місцем злочину тощо. «OSINT» є продуктивною системою протидії злочинам які відбуваються у кіберпросторі, треба лише правильно використовувати цей метод, враховуючи міжнародний досвід.

Одним з методів збирання оперативної інформації є використання розвідки з відкритих джерел, а саме «OSINT» (open-source intelligence). Сьогодні можна спостерігати збільшення зацікавленості в OSINT не лише з боку журналістів, аналітиків приватних компаній та пересічних громадян, але й аналітиків спецслужб, тому що «OSINT» має певні переваги перед збором, обробкою та аналізом інформації з обмеженим доступом, на сам перед тому, що не вимагає спеціального доступу до інформації, а значить зберігає час користувача, не вимагає спеціальних навичок, витрат значних коштів. Використання «OSINT» в деяких випадках дає змогу запобігти вчиненню злочинну, адже вираз «Краще попередити злочин, ніж карати» здобуває все більшого значення.

«OSINT» (Open Source INTelligence) – це збір, аналіз, обробка даних які знаходяться у загальному доступі, але ці данні завжди специфічні, тобто зібрані та структуровані особливим способом, задля відповіді на конкретне питання [1]. У 1947 році аналітик ЦРУ Кен Шерман зазначив що держава отримує з відкритих джерел інформації майже 80 %, пізніше (генерал-лейтенант, керівник Розвідувального управління міністерства оборони США) Самуель Уілсон стверджував

що 90 % всієї розвідувальної інформації надходить з відкритих джерел, а лише 10 % – з роботи агентури [2, с. 62].

Найширше використання «OSINT» здобув у США. Можна навести перелік організацій які користуються цим методом:

– Рада із захисту відкритих джерел (DOSC);

– Командування розвідки і безпеки ЗС США (INSCOM);

– Служба розвідувальної інформації Департаменту сухопутних військ (DA IIS);

– Національна розвідка центру відкритих джерел (DNI OSC);

– Академія відкритих джерел;

– Департамент передових систем (ASD);

– ФБР;

– Дослідницька служба бібліотеки Конгресу (Congressional Research Service).

США використовує інформацію, отриману за допомогою «OSINT», в більшій мірі для планування бойових дій, організації та проведення військових операцій, запобігання терористичним актам [2, 3]. На думку аналітиків розвідки США найбільшою проблемою методу «OSINT» на даний момент є неперевірені джерела інформації, провокуючі ресурси, недостовірна інформація. Для отримання найбільш актуальної та якісної інформації користувач повинен обробити багато інформації з різних джерел та узагальнити її так, як вимагає мета та завдання дослідження.

У США сформована розгалужена мережа центрів і пунктів, що ведуть OSINT-розвідку та надають відомості більш ніж 7 тис. споживачам розвідувальних даних. І це не що інше, як результат скоординованих дій законодавчої і виконавчої влади, спрямованих на проведення цілеспрямованої політики в галузі забезпечення національної безпеки. Подібні структури є на всіх рівнях [4].

Ізраїль також використовує «OSINT» в першу чергу для аналізу військової спроможності противника. В структурі військової розвідки існує окремий спеціальний підрозділ для аналізу відкритих джерел інформації «Hatsaf», який збирає інформацію лише для військових цілей.

У Великобританії за допомогою «OSINT» цивільні журналісти служби BBC Monitoring здійснюють первинний збір інформації, яка в подальшому потрапляє до співробітників спецслужб для її використання за конкретними напрямами досліджень.

Зважаючи на міжнародний досвід використання «OSINT» можна зазначити, що для отримання якісної та актуальної інформації необхідно опрацьовувати велику кількість інформаційних джерел. Для

правильної та продуктивної роботи цього методу не достатньо лише знаходити інформацію, її треба обробляти, аналізувати, знаходити підтвердження досліджуваних фактів, подій та явищ, адже багато інформації створюється саме для дезінформації.

На сьогоднішній день в провідних країнах світу «OSINT» активно та успішно використовується інформаційно-аналітичними підрозділами; дані відсоткового співвідношення продуктивності відкритих джерел інформації підтверджують необхідність та актуальність використання досвіду США та країн Європи для вирішення оперативних, тактичних та стратегічних завдань силових структур.

Оскільки різниця між новачком, який шукає в Інтернеті інформацію і OSINT-професіоналом, який обізнаний з методикою пошуку та аналізу, має певні навички у цій сфері, колосальна: там, де новачок побачить фото, кількість репостів, групи і сторінки, на які підписана людина, профіль особи у соціальних мережах, – професіонал побачить активність, дати публікацій, фон на фотографіях, можливі причини підписки на певні групи, виділить кола спілкування (побудує схему зв'язків особи/осіб) тощо.

Отже ключовими факторами для успішного аналізу є:

– чітке розуміння цілей аналізу;

– неупередженість (максимальна об'єктивність аналітика);

– збір інформації з максимально можливої кількості відкритих джерел;

– застосування «коефіцієнтів ваги» до кожної інформації;

– чіткість представлення даних;

– грамотний аналіз отриманої інформації.

Список бібліографічних посилань

1. Политическое Экспертное Сообщество (Модель OSINT. Открытые источники в мире разведки) URL: http://strateger.net/model_osint_otkritie_istochniki_v_mire_razvedki (дата звернення: 29.10.2018).

2. Распознавание информационных операций / А. Г. Додонов, Д. В. Ландэ, В. В. Цыганок, О. В. Андрейчук, С. В. Каденко, А. Н. Грайворонская. К. : ООО «Инжиниринг», 2017. 282 с.

3. Разведка с использованием открытых источников информации в США. URL: http://pentagonus.ru/publ/razvedka_s_ispolzovaniem_otkrytykh_istochnikov_informacii_v_ssha/80-1-0-1614 (дата звернення: 29.10.2018).

4. Разведка на основе открытых источников. URL: http://www.in4sec.com.ua/razvedka-na-osnove-otkry-ty-h-istochnikov-open-source-intelligence-osint/ (дата звернення: 29.10.2018).

Одержано 31.10.2018