Максим ВОРОБЙОВ
курсант ІІ курсу факультету № 1 Криворізького навчально-наукового інституту Донецького державного університету внутрішніх справ
Науковий керівник:
Тетяна ПАВЛИШ
доцент кафедри спеціальних дисциплін та професійної підготовки факультету № 1 Криворізького навчально-наукового інституту Донецького державного університету внутрішніх справ, кандидат педагогічних наук

ПЕРСПЕКТИВИ ТА ПРАКТИКА ВИКОРИСТАННЯ OSINT В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

В епоху глобалізації та стрімкого розвитку інформаційних технологій наше життя стає більш комфортним та зручним. Інформаційні технології дозволяють нам отримувати швидкий та безперешкодний доступ до інформації, послуг та товарів, що зробило нашу взаємодію між людьми та організаціями більш ефективними та зручними на всіх рівнях.

Але, злочинний світ також не стоїть на місці. Злочинці пристосовуються до швидкого розвитку інформаційних технологій та намагаються використовувати їх для власних цілей. Інтернет, соціальні мережі та інші технології стали незамінними інструментами для правопорушників, які використовують їх для розповсюдження фейкових новин, крадіжок особистої інформації та ідентифікаційних даних, шахрайства та інших видів кіберзлочинності.

У сучасному світі, інформація є ключовим ресурсом для розвитку і успіху будь-якої сфери життя. На одному боці стоять правоохоронні органи, які мають за мету захист прав громадян та забезпечення правопорядку. Але на другому боці - злочинний світ, який також має доступ до інформації та використовує її для своїх цілей, таких як шахрайства, кібератаки та кібершпигунство. За таких умов, правоохоронні органи повинні постійно бути на крок попереду від

злочинців.

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 інтернетбезпеки та ін. [1]

Формування даного поняття відбувалося шляхом трансформації поняття «інформація з відкритих джерел» (open source information (OSIF). У спрощеному варіанті, даний термін стосується інформації, що не має грифу «таємно». Розвідувальне співтовариство США (Intelligence Community) визначає таку інформацію як загальнодоступний матеріал, що може отримати кожен законним шляхом через запит, купівлю чи спостереження. Збір такої інформації повинен відповідати діючим вимогам захисту авторських прав [2]

Відкриті джерела інформації можна розділити на 4 категорії:

1. широко розповсюджені дані та інформація;

2. цільові комерційні дані;

3. експертні оцінки;

4. «сіра» література

Хоча Національна поліція має невеликий досвід використання методів відкритих джерел інформації (OSINT), можна скористатися міжнародним досвідом використання цих методів для практичного застосування.

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 [3].

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 [3].

В публікації міжнародної волонтерської спільноти InformNapalm демонструється, як можна перевірити інформацію щодо втрат Збройних Сил

російської федерації, яка з’явилася в мережі Інтернет. Зокрема, за даними Міністерства оборони рф станом на 24.03.2022 було вбито 498 і поранено 1597 осіб. Аналіз повідомлень з російських ЗМІ та соціальних мереж, що проводили волонтери InformNapalm, свідчить про нагородження російських військових, які брали участь у війні з Україною, посмертно Орденом Мужності. З урахуванням мінімального та максимального номеру цієї нагороди, можна стверджувати, що загальна кількість загиблих військовослужбовців ЗС рф є не меншою за 4794 особи [4].

Використання OSINT (відкритих джерел) може бути дуже перспективним для Національної поліції України в багатьох напрямках.

По-перше, це може допомогти поліції отримувати оперативну інформацію про злочини та злочинців, зокрема за допомогою моніторингу соціальних мереж та інших відкритих джерел.

По-друге, використання OSINT може допомогти в розслідуванні злочинів та зборі доказів у кримінальних справах. Наприклад, аналіз відкритих джерел може дати можливість встановити місцезнаходження підозрюваних, знайти свідків та іншу корисну інформацію.

По-третє, використання OSINT може допомогти у попередженні злочинів, зокрема шляхом моніторингу соціальних мереж та відслідковування наявності загроз безпеці громадян.

Однак, для успішного використання OSINT необхідно володіти відповідними навичками та знаннями, тому важливо забезпечити необхідне навчання та підготовку спеціалістів Національної поліції. Також важливо забезпечити належний захист персональних даних та інших конфіденційних даних під час збору та обробки інформації з відкритих джерел.

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-konkurentnoirozvidki-st-51-68 (дата звернення 24.04.2023)

2. Open Source Intelligence (OSINT): Issues for Congress, December 5, 2007. URL: www.fas.org/sgp/crs/intel/RL34270.pdf (дата звернення 24.04.2023)
3. Міжнародний досвід використання OSINT. URL: https://dspace.univd.edu.ua/items/dfc25df1-9200-424c-be8f-1cabe44037f2 (дата звернення 24.04.2023)
4. «Медальний залік»: OSINT аналіз справжніх втрат РФ за перший тиждень бойових дій в Україні. URL: https://informnapalm.org/ua/medalnyizalik-analiz-osint/ (дата звернення 24.04.2023)

Єлизавета ШАЄЦ
курсантка 1 курсу факультету № 3 Донецького державного університету внутрішніх справ
Науковий керівник:
Ольга ЛУНГОЛ
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету № 3 ДонДУВС, к.п.н.

КІБЕРПРОСТІР ЯК КВІНТЕСЕНЦІЯ ГЛОБАЛІЗОВАНОГО СУСПІЛЬСТВА

Кіберпростір як квінтесенція глобалізованого суспільства відображає сутність сучасної світової спільноти, де технології та Інтернет переплітаються з усіма сферами життя. Він стає цифровим простором, де здійснюється взаємодія між людьми, організаціями та системами. Кіберпростір забезпечує безперервний потік інформації, комунікацію та доступ до різноманітних ресурсів. Це глобальне кіберсередовище стало ареною для реалізації економічних, соціальних, політичних та культурних процесів. Кіберпростір пронизує всі сфери життя, включаючи комерцію, освіту, державну адміністрацію, медицину, науку тощо.

В ЗУ «Про основні засади забезпечення кібербезпеки України» надано