УДК 342.1
DOI https://doi.org/10.24144/2307-3322.2024.82.2.28

ЗАРУБІЖНИЙ ДОСВІД АНТИТЕРОРИСТИЧНОГО ВИКОРИСТАННЯ OSINT

Користін О.Є.,
доктор юридичних наук, професор,
заслужений діяч науки і техніки України,
ЦСК ННІ ІБСК НА СБ України
ORCID: https://orcid.org/0000-0001-9056-5475

Свиридюк Н.П.,
доктор юридичних наук, професор;
Одеський державний університет внутрішніх справ,
ЦСК ННІ ІБСК НА СБ України
ORCID: https://orcid.org/0000-0001-9772-1119

Користін О.Є., Свиридюк Н.П. Зарубіжний досвід антитерористичного використання OSINT.

До завдань правоохоронних органів входить підтримання правопорядку, захист громадян, запобігання, виявлення та розслідування злочинів. Одним з найважливіших аспектів успішної поліцейської роботи є здатність поліції отримувати своєчасну, достовірну і дієву розвідувальну інформацію, пов'язану з розслідування правопорушення. OSINT може надати органам правопорядку і безпеки критично важливу можливість доповнити і посилити свої розвідувальні можливості, оскільки здатність швидко збирати і точно обробляти та аналізувати дані з відкритих джерел може бути суттєвою допомогою під час розслідувань, а також використовуватися для стратегічного планування боротьби зі злочинністю на національному рівні. OSINT додатково до матеріалів кримінального провадження забезпечує безцінний спосіб доступу до інформації та її збору з відкритих джерел, до даних про місцезнаходження, а також комбінується з аналітичними можливостями в реальному часі. Таким чином, цілеспрямований та законний моніторинг, аналіз та візуалізація даних з відкритих джерел має розглядатися як обов'язкова вимога будь-якої стратегії національної безпеки.

У контексті використання OSINT, підвищення його потенціалу та ефективності, важливим є вивчення зарубіжного досвіду, зокрема, розробленої стратегії Великої Британії – CONTEST, яка є основою для заходів із запобігання терору, переслідування терористів та захисту від тероризму загалом. Результати та досягнення ефективних й інноваційних рішень органів безпеки та правопорядку розглянуто і у контексті співпраці з приватними та державними партнерами, в тому числі з науковими колами. Використовуючи успішний досвід Центру OSINT (CENTRIC OSINT Hub), зазначено, що наукові кола та правоохоронні органи можуть співпрацювати у сфері OSINT для того, щоб втілити дослідження в реальність задля безпеки та захисту громадян.

Ключові слова: тероризм, OSINT, розвідка з відкритих джерел, аналітична розвідка, розслідування, правоохоронні органи.

Korystin O.E., Svyrydiuk N.P. Foreign Experience in the Anti-Terrorist Use of OSINT.

The tasks of law enforcement agencies include maintaining law and order, protecting citizens, preventing, detecting and investigating crimes. One of the most important aspects of successful police work is the ability of the police to obtain timely, reliable and effective intelligence information related to the investigation of an offense. OSINT can provide law enforcement and security agencies with a critical opportunity to supplement and enhance their intelligence capabilities, as the ability to quickly collect and accurately process and analyze open source data can be a significant aid to investigations, as well as used for strategic planning of crime fighting at the national level. OSINT, in addition to criminal proceedings, provides an invaluable way to access and collect information from open sources, location

data, and combines it with real-time analytical capabilities. Thus, targeted and legitimate monitoring, analysis and visualization of open source data should be considered a mandatory requirement of any national security strategy.

In the context of using OSINT, increasing its potential and effectiveness, it is important to study foreign experience, in particular, the developed UK strategy - CONTEST, which is the basis for measures to prevent terrorism, prosecute terrorists and protect against terrorism in general. The results and achievements of effective and innovative solutions by security and law enforcement agencies are also considered in the context of cooperation with private and public partners, including academia. Using the successful experience of the CENTRIC OSINT Hub, it is noted that academia and law enforcement agencies can cooperate in the field of OSINT in order to translate research into reality for the safety of citizens.

Key words: terrorism, OSINT, Open Source Intelligence, Intelligence, investigation, law enforcement agencies.

Постановка проблеми. Широке використання правоохоронними органами та органами державної безпеки аналітичної розвідки (Intelligence) [1; 2] і особливо розвідки з відкритих джерел (Open Source Intelligence – OSINT) відбувається на тлі конфліктів, нестабільності, поширення насильства в різних регіонах світу. Україна не є виключенням, сучасні інструменти пошуку та аналізу інформації особливо актуальними для органів безпеки та правопорядку стали в умовах широкомасштабної агресії рф, посягання на її державний суверенітет та територіальну цілісність.

Обробка великої кількості інформації в OSINT може бути викликом через обсяг даних, які потрібно аналізувати. Щоб ефективно обробляти великі обсяги інформації в рамках OSINT, створюються інструменти, які можуть сприяти цьому процесу. Вони значно полегшують процес обробки великої кількості інформації та дозволяють здійснювати більш ефективний та точний аналіз даних [3]. Також, вони надають можливості для створення комплексних звітів та аналітичних висновків, що допомагає аналізувати інформацію з різних сторін та отримувати більше контексту для прийняття важливих рішень.

Водночас не втрачається актуальність вивчення досвіду розвинених країн світу, які мають можливість більшого зосередження ресурсів та забезпечення на цій основі інноваційного розвитку цього напряму аналітичного процесу у сфері безпеки та правопорядку. Наразі, Велика Британія, як і багато інших країн, перебуває під постійною загрозою реальних і потенційних атак з боку різноманітних небезпек, включаючи організовану злочинність, кіберзагрози та тероризм, які – якщо їх не зупинити – можуть завдати надзвичайної шкоди громадянам, громадам та державам у цілому.

Метою цієї статті є дослідження окремих напрямів використання OSINT у сфері національної безпеки, зокрема антитерористичного характеру, окреслення їх змісту й характеристики на основі досвіду Великої Британії.

Виклад основного матеріалу. Масштаб і рівень жорстокості терористичних атак, таких як у Парижі, Брюсселі, Ніцці та Мюнхені є холодним і відчутним нагадуванням про дуже реальну загрозу, з якою стикаються різні нації у всьому світу. Одним із загальних чинників, що простежується в тому, як ці загрози реалізуються, є використання інтернет-платформ для спілкування терористами або окремими групами, такими як самопроголошена Ісламська держава. Наприклад, соціальні мережі все частіше стають домінуючою платформою для впливу на іноземних громадян, насамперед через поширення пропаганди, складних методик рекрутингових кампаній [4], маніпулюючи з безпрецедентною простотою та використовуючи доступ до вразливих груп населення. Наразі, мають місце певні статистичні дані, що відображають залучення великої кількості іноземних громадян, які беруть участь у бойових діях в Іраку та Сирії [5], а також арешти та ув'язнення британських дітей віком від 14 до 17 років за заохочення та організацію терористичних атак [6; 7].

Протягом останніх років OSINT все частіше використовується організаціями приватного сектору як засіб вимірювання лояльності клієнтів, відстеження громадської думки та оцінки сприйняття продукту. Аналогічно, органи державної безпеки та правопорядку визнають необхідність застосування подібних методів для посилення своїх слідчих можливостей та покращення здатності виявляти й реагувати на кримінальні загрози. Кримінальні суб'єкти використовують інтернет для вербування, створення незаконних картелів, передачі інформації та коштів для фінансування та координації своєї незаконної діяльності [8].

Поширення інтернету переплело континенти, культури і спільноти, а також інтегрувало більшість сучасних технологій. Хоча соціальні мережі залишаються домінуючою онлайн-платформою для кримінальної та екстремістської активності, існує все більша ймовірність того, що вони підуть шляхом інтернету, розгалужуючись, використовуючи ігрові консолі [9], мобільні додатки [10], хмарні сховища [11] та інші технології. У той час як соціальні медіа та відкритий інтернет використовуються в основному для психологічної, моральної та емоційної тактики, темна мережа (Dark Web) більшою мірою використовується для фізичної і тактичної сторони операцій, зосереджуючись на зброї та боєприпасах [12], фальшивих документах [13], виготовленні вибухових пристроїв, криптовалютному фінансуванні [14] та зашифрованих анонімних стратегічних комунікаціях.

Повсюдне поширення інтернету значно збільшило кількість, цінність і доступність джерел OSINT. За визначенням, OSINT - це розвідка, заснована на інформації, яка знаходиться у вільному доступі з відкритих джерел, таких як газетні повідомлення журналів, радіо- і телепередач, а в сучасних умовах - все частіше соціальних мереж та інтернету [8].

При роботі з розвідувальними даними, отриманими з відкритих джерел, а саме соціальними мережами, існує вимога дотримання конфіденційності та фундаментальних принципів щодо прав людини керувати, незважаючи на те, що багато інформації, розміщеної на таких сайтах, як Facebook і Twitter, часто знаходиться у вільному доступі, але зареєстровані користувачі вважають її особистою. При роботі з OSINT, на відміну від більш традиційних закритих розвідувальних джерел розвідувальної інформації, інтереси розвідувального співтовариства зміщується з доступності інформації до ідентифікації релевантної й точної інформації. З цих причин все частіше виникає необхідність перевіряти розвідувальні дані, отримані з відкритих джерел, з розвідданими з надійних, закритих джерел і досвідом фахівців з безпеки [8]. Перевірка розвідданих таким чином є особливо гострою темою, коли йдеться про контент у соціальних мережах, оскільки користувачі часто вирішують не розкривати або фальсифікувати особисту інформацію, яку вони надають на цих платформах [15].

З точки зору національної безпеки, рішення на основі OSINT мають посилити можливості органів безпеки та правопорядку, надаючи доступ до більш дієвих розвідувальних даних, які можуть підтримати існуючі процеси прийняття рішень, постановки завдань та координації діяльності. Ядро будь-якого OSINT-рішення має бути зосереджене на зборі та використанні даних, орієнтованих на інтернет. Останнє включає в себе розробку розширених можливостей і сервісів для збору, аналізу, візуалізації та об'єднання відповідних даних, на основі яких можна генерувати динамічні гіпотези в реальному часі.

Заходи боротьби зі злочинністю і тероризмом - онлайн і офлайн - стають все більш важливим елементом будь-якої стратегії національної безпеки. Дивлячись на сучасні підходи до боротьби з тероризмом у Великій Британії, ключові принципи стратегії CONTEST [16] забезпечують фундаментальну основу заходів із запобігання тероризму, переслідування підозрюваних, захисту громадян і формування готовності до терору.

Слід зазначити, що хоча цілі терористів і організованих злочинних угруповань відрізняються, зв'язки між терористичною і організованою злочинною діяльністю, схоже, зростають. Наприклад, під час теракту в Мюнхені (22 липня 2016 р.) вважається, що виконавець нападу придбав зброю через «Dark Web». Злочинна діяльність, до якої залучені терористичні групи, або через зв'язки з окремими злочинцями і злочинними угрупованнями, або через власні операції, може включати торгівлю незаконними товарами і речовинами, такими як зброя і наркотики, торгівлю людьми, фінансове шахрайство, відмивання коштів і вимагання [8].

OSINT вже використовується як одне з ключових джерел розвідданих для національної безпеки, і його значення тільки зростає. Спектр поточних і потенційних застосувань є величезним. Однак, OSINT не може бути єдиним джерелом, на яке покладаються правоохоронні органи. OSINT є ефективним, коли він здатен доповнити існуючі розвідувальні дані з професійних, відомчих або закритих джерел, надаючи додаткову інформацію та вказуючи напрям подальшої аналітичної розвідки [8].

Перспективним підходом до забезпечення ефективних та інноваційних рішень і процесів є співпраця між різними державними і приватними суб'єктами та організаціями, такими як, наприклад, органів державної безпеки та правопорядку, бізнесових та наукових фахових осередків. Для прикладу, цей напрям (OSINT Hub) реалізовано у Центрі передового досвіду досліджень з питань

тероризму, стійкості, аналітичної розвідки та організованої злочинності (Centre of Excellence for Terrorism, Resilience, Intelligence and Organized Crime Research), з узагальненою назвою CENTRIC.

З 2012 року CENTRIC створив потужний науково-дослідний потенціал, зосереджений на оперативному використанні OSINT в контексті його застосування щодо боротьби з тероризмом, кіберзлочинністю, кризового менеджменту, а також ідентифікації та моделювання організованої злочинності.

На початку 2016 року CENTRIC запустив, так званий, OSINT Hub, який набирає обертів як фізичний і віртуальний простір для оперативного використання, поширення і розвитку можливостей CENTRIC. Такі можливості постійно розвиваються і вдосконалюються на основі нових знань та інструментарію. Це відбувається у тісній співпраці з науковими колами, національними, загальноєвропейськими та міжнародними партнерами, державним та приватним секторами. Експертне залучення реалізовано в OSINT Hub на основі прямої співпраці з низкою правоохоронних органів та слідчими групами, що безпосередньо впливають на роботу хабу та розширюють його можливості [16].

Основою для ситуаційної обізнаності та можливостей обробки даних OSINT Hub стала участь Центру у великих проектах ЄС у співпраці з правоохоронними органами та іншими міжнародними організаціями в якості основного технічного партнера відповідального за надання інформаційної ситуаційної обізнаності, веб-сканування, виявлення суб'єктів веб-пошуку, виявлення об'єктів, категоризації контенту, соціальних мереж та функцій агрегації даних – все це побудовано на найсучасніших інструментах, які пропонуються провідними провайдерами, спільнотами у відкритих джерелах та існуючими академічними дослідженнями. Використання цих можливостей дозволило CENTRIC більш ефективно здійснювати обробку даних і управління партнерським середовищем. На сьогоднішній день OSINT Hub надав підтримку в проведенні різних розслідувань, починаючи від сексуальної експлуатації дітей до тероризму [8].

Безпечне фізичне середовище в OSINT Hub дозволяє слідчим працювати безпосередньо з командою CENTRIC та їхніми інструментами і робити безпосередній внесок у розробку майбутніх можливостей. Багато з можливостей OSINT Hub для проведення розслідувань були сформовані завдяки такій співпраці й принесли очевидну користь правоохоронним органам завдяки скороченню витрат як на цільові розслідування, так і на стратегічну ситуаційну обізнаність. Використовуючи інструменти Центру, досліджується також потенціал OSINT, забезпечуючи сумісність з існуючими системами управління і процесами, а також дотримання існуючих управлінських і правових вимог, таких як RIPA та Закону про захист даних [8].

Висновки. Функції правоохоронних органів включають підтримання правопорядку, захист громадян, а також запобігання, виявлення та розслідування злочинів. Досягаючи цих цілей, правоохоронні органи виконують функцію захисту безпеки суспільства та громадян, яким вони служать. OSINT потенційно може надати органам державної безпеки та правопорядку критично важливі можливості для доповнення та посилення їхніх розвідувальних можливостей. Цілеспрямований і законний моніторинг, аналіз і візуалізація публічних відкритих джерел даних повинні розглядатися як обов'язкові вимоги будь-якої стратегії національної безпеки. Здатність швидко збирати, точно обробляти та аналізувати дані з відкритих джерел може стати значною допомогою під час розслідувань, а також може бути використана для стратегічного планування боротьби зі злочинністю на національному рівні, зокрема й тероризму. Однак для досягнення ефективних та інноваційних рішень, правоохоронним органам може бути доцільно розглянути можливість співпраці з приватними та державними партнерами, зокрема науковими колами. Успішна реалізація OSINT Hub проєктом CENTRIC є прикладом того, як науковці та правоохоронні органи можуть співпрацювати у сфері OSINT для того, щоб втілити дослідження в реальність задля безпеки і захисту громадян.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Користін О.Є., Денисенко Б.А. Зміст та інтерпретація терміна «intelligence» в контексті моделі Intelligence-led policing (ILP). *Південноукраїнський правничий часопис*. № 1. 2023. С. 72–79. DOI https://doi.org/10.32850/sulj.2023.1.13.
2. Користін О., Денисенко Б. Розділ 23. Методологічні засади OSINT. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України:

монографія / Користін О., Швець Д., Бутко Б., Денисенко Б. та ін., за заг. ред. Користіна О.Є. Київ: «ВАЙТ», 2024. 504 с. С. 371–383.
3. Ісмайлов К., Пєфтієв Д. Розділ 16. Цифрові технології та аналітичні засоби аналізу воєнних злочинів в Україні. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України: *монографія* / Користін О., Швець Д., Бутко Б., Денисенко Б. та ін., за заг. ред. Користіна О.Є. Київ: «ВАЙТ», 2024. 504 с. С. 253–267.
4. Helmus, T.C., York, E., Chalk, P. (2013). Promoting Online Voices for Countering Violent Extremism. (Rand Corporation, Santa Monica, California). URL: http://www.rand.org/ pubs/research_reports/RR130.html.
5. Bartlett, E. (2014). Record number of foreign nationals fighting in Iraq and Syria. The Independent Online. URLt: http://indy100.independent.co.uk/article/record-number-of-foreign-nationals-fighting-in-iraq-and-syria–gk2635auox.
6. BBC. (2015). Anzac Day terror plot: Blackburn boy sentenced to life. URL: http://www.bbc.co.uk/news/uk-34423984.
7. Dodd, V. (2016). Counter-terrorism detectives arrest east London teenager. The Guardian Online. URL: https://www.theguardian.com/uk-news/2016/jun/16/counter-terrorism-detectives-arrest-east-london-teenager.
8. Babak Akhgar, Saskia Bayerl, Fraser Sampson (2016). Open source intelligence Investigation: from strategy to implementation. Cham CH: Springer.
9. Tassi, P. (2015). How ISIS terrorists may have used PlayStation 4 to discuss and plan attacks. Forbes Online. URL: http://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isisterrorists-used-ps4-to-plan-attacks/#39d5c755731a.
10. Billington, J. (2015). Paris terrorists used WhatsApp and Telegram to plot attacks according to investigators. International Business Times. URL: http://www.ibtimes.co.uk/ paristerrorists-used-whatsapp-telegram-plot-attacks-according-investigators-1533880.
11. Hall, K. (2011). Cyber terrorism set to increase after al-Qaeda calls for more cyber-attacks, says government. Computer Weekly Online. URL: http://www.computerweekly.com/news/2240105012/Cyber-terrorism-set-to-increase-after-al-Qaeda-calls-for-more-cyber-attacks-saysgovernment.
12. DeepDotWeb. URL: https://www.deepdotweb.com/tag/guns/.
13. Charlton, A. (2015). Dark web vendors sell blank British passport and entry to database for just £2000. URL: http://www.ibtimes.co.uk/dark-web-vendors-sell-blank-british-passportsentry-passport-database-just-2000-1509564.
14. Smith, M. (2015). Hacktivists claim ISIS terrorists linked to Paris attacks had bitcoin funding. Network world. URL: http://www.networkworld.com/article/3005308/security /hacktivists-claimisis-terrorists-linked-to-paris-attacks-had-bitcoin-funding.html.
15. Bayerl, P.S., Akhgar, B. (2015). Surveillance and falsification implications for open source intelligence investigations. *Commun ACM*, 58 (8): 62–69.
16. Contest Strategy (2011). The UK's strategy for countering terrorism, Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, July 2011.