НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

КРУГЛИЙ СТІЛ

АКТУАЛЬНІ ПИТАННЯ ВИКОРИСТАННЯ МЕТОДІВ І ЗАСОБІВ OSINT У РОБОТІ ПІДРОЗДІЛІВ ЗАХИСТУ НАЦІОНАЛЬНОЇ ДЕРЖАВНОСТІ

(М. КИЇВ, 31 БЕРЕЗНЯ 2023 РОКУ)

ЗБІРНИК МАТЕРІАЛІВ
(ЧАСТИНА 1)

КИЇВ
2023

СЛУЖБА БЕЗПЕКИ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ДЕРЖАВНОЇ БЕЗПЕКИ
ЦЕНТР ЗАХИСТУ НАЦІОНАЛЬНОЇ ДЕРЖАВНОСТІ

АКТУАЛЬНІ ПИТАННЯ ВИКОРИСТАННЯ МЕТОДІВ І ЗАСОБІВ OSINT У РОБОТІ ПІДРОЗДІЛІВ ЗАХИСТУ НАЦІОНАЛЬНОЇ ДЕРЖАВНОСТІ

Збірник матеріалів круглого столу
(м. Київ, 31 березня 2023 року)

Частина 1

Київ
2023

УДК 355.40 (06)
А43

Рекомендовано до друку Вченою радою
Навчально-наукового інституту державної безпеки
Національної академії Служби безпеки України
(протокол № 5 від 31 травня 2023 року)

А43 **Актуальні** питання використання методів і засобів OSINT у роботі підрозділів захисту національної державності : зб. матер. круглого столу (м. Київ, 31 березня 2023 р.) : у 2-х ч. Ч. 1. Київ : НА СБУ, 2023. 75 с.

У збірнику матеріалів круглого столу розміщені тези доповідей з обговорення актуальних питань використання методів і засобів OSINT, як у роботі підрозділів захисту національної державності й інших контррозвідувальних підрозділів Служби безпеки України, так і в роботі суб'єктів сектору безпеки і оборони України, досвід яких може бути використаний для покращення ефективності оперативно-службової діяльності Служби безпеки України.

З урахуванням того, що сучасний стан розвитку української держави в умовах воєнного стану характеризується наявністю нових викликів і загроз серед напрямів круглого столу висвітлені питання взаємодії органів і підрозділів Служби безпеки України з іншими суб'єктами сектору безпеки держави, органами влади та управління, громадянським суспільством з захисту державного суверенітету, конституційного ладу і територіальної цілісності України.

Для співробітників Служби безпеки України, суб'єктів сектору безпеки і оборони України, інших державних і правоохоронних органів, наукового і науково-педагогічного складу, фахівців із безпеки і державного управління. Матеріал друкується в авторській редакції.

УДК 355.40 (06)

ВІТАЛЬНЕ СЛОВО
ректора Національної академії Служби безпеки України, доктора юридичних наук, доцента Андрія ЧЕРНЯКА

Доброго дня, шановні учасники круглого столу!

Радий вітати вас в Національній академії Служби безпеки України, котра знову об'єднала представників науки і практики, стала майданчиком для обговорення та подальшого вирішення нагальних питань практичного використання інформації, отриманої з використанням методів та засобів OSINT у контексті відбиття військової агресії росії.

На сьогодні особливої актуальності набуває взаємодія державних і правоохоронних органів з громадським сектором заради забезпечення державної безпеки нашої країни, що обговорюватимемо з представниками Центрального управління, регіональних органів Служби безпеки України та науковою спільнотою.

Результати розвідки з відкритих джерел активно використовуються як для встановлення конкретних координат розташування ворога для ураження українськими військовими формуваннями, так і для документування воєнних злочинів агресора та конкретних осіб, причетних до їх вчинення. Значний внесок у цю благородну справу привносять присутні тут працівники наукових установ і навчальних закладів, громадських організацій, військових, спеціальних й правоохоронних органів, які розробляють теоретичну та практичну методику проведення розвідки, досягаючи вагомих конкретних здобутків.

На нашому форумі присутні гості з Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Національного авіаційного університету, Національного юридичного університету імені Ярослава Мудрого, Національної академії внутрішніх справ, Національної академії Національної гвардії України, Національної академії Державної прикордонної служби України імені Богдана Хмельницького, Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Інституту підготовки юридичних кадрів для Служби безпеки України Національного юридичного університету імені Ярослава Мудрого, Навчально-наукового інституту «Інститут державного управління» Харківського на-

ціонального університету імені В.Н. Каразіна та інших навчальних і наукових закладів України.

Мої вітання представникам дослідницьких структур OSINT-спільноти громадських організацій «Інститут постінформаційного суспільства», «Мольфар», «YouControl» та інших, які впродовж тривалого часу, а особливо, з початком відкритої агресії рф проти нашої держави, здійснюють ефективну співпрацю з Національною академією СБ України, організовуючи проведення тренінгів та навчальних курсів для курсантів та співробітників академії з питань теоретичних засад та практичного застосування методів і засобів OSINT.

Сподіваємося, що присутні у цій залі та в онлайн-форматі співробітники органів і підрозділів Служби безпеки України ще активніше впроваджуватимуть у свою діяльність методики розвідки з відкритих джерел, спираючись на міжнародний досвід та напрацювання вітчизняних дослідників.

Бажаю плідної роботи всім учасникам Круглого столу задля майбутньої перемоги! Слава Україні!

ВІТАЛЬНЕ СЛОВО
представника Апарату Голови Служби безпеки України Людмили КУЛЬЧИЦЬКОЇ

Шановний пане ректоре,
панове офіцери та учасники круглого столу!

Насамперед, дякую за можливість участі в такому непересічному і без сумніву важливому заході.

Розвідка з відкритих джерел (а саме так перекладається Open Source Intelligence (OSINT)) – не нове явище в діяльності Служби безпеки України та спеціальних служб.

Як кажуть наші зарубіжні колеги, суть роботи з відкритими джерелами – незмінна вже десятки років, однак змінилися технології. І змінилися вони настільки, що OSINT став справою далеко не виключно спецслужб.

Кількість даних, що циркулюють в мережі Інтернет, вражає. Аналітики «The Economist» підрахували, що за 10 років війни у Сирії в Мережі було розміщено відео тривалістю 40 років. І такої ж довжини відео – 40 років – потрапило в мережу тільки за 80 днів з початку повномасштабного вторгнення росії.

Зрозуміло, що жодна структура, якою б потужною вона не була, не опрацює таку кількість інформації самостійно.

Надзвичайна синергія – співпраця громадськості, суспільства і державних структур, збройних сил – у боротьбі з загарбниками стала запорукою успішної протидії повномасштабному вторгненню в 2022 році. І стосується це не тільки ведення воєнних дій, а й інформаційної сфери.

І ця ж синергія, вірю, стане запорукою нашої Перемоги і притягнення до відповідальності всіх воєнних злочинців – від солдат і офіцерів до політичного керівництва країни-агресора. Ми всі над цим працюємо, кожен у своїй сфері і водночас разом.

Майже рік тому, на початку квітня 2022 року, саме тут – в Академії – відбулася нарада за участі офіцерів і курсантів СБ України. Однією з тем наради була робота з відкритими джерелами для доопрацювання найгарячішої інформації, яка надходила з деокупованої Київщини. Хочеться ще раз висловити слова подяки кожному курсанту і кожному офіцеру, з ким ми працювали пліч-о-пліч.

Тому зараз, сьогодні, ми вітаємо кожну можливість обміну досвідом, збагачення новими знаннями за участі і співробітників Служби безпеки України, і представників громадських організацій, фахівців з OSINT, та, звичайно, для створення тієї самої синергії, завдяки якій ми переможемо ворога.

Слава Україні!

Шепітько В. Ю.
доктор юридичних наук, професор,
академік НАПрН України
Шепітько М. В.
доктор юридичних наук, старший науковий співробітник,
Національний юридичний університету
імені Ярослава Мудрого

РОЛЬ ЦИФРОВОЇ КРИМІНАЛІСТИКИ У ДОКАЗУВАННІ ФАКТІВ ВЧИНЕННЯ ВОЄННИХ ТА ІНШИХ МІЖНАРОДНИХ ЗЛОЧИНІВ І МОЖЛИВОСТІ ВИКОРИСТАННЯ ПРОТОКОЛУ БЕРКЛІ

Використання цифрової інформації (цифрових доказів) набуває першорядного значення в умовах здійснення повномасштабної війни Росії проти України. Російська федерація веде проти України повномасштабну війну, яка змусила більше ніж третину українців покинути свої домівки (майже 14 мільйонів українців за перші 100 днів війни), а у багатьох забрала й життя. За даними Управління Верховного комісара ООН у справах біженців встановлено, що в Європі перебувало 7,6 мільйонів українських біженців, 4,2 мільйона зареєструвалися та попросили прихисток та допомогу [1].

Способами ведення цієї війни є цілеспрямований терор в усіх українських регіонах, масові вбивства та катування, викрадення людей та зґвалтування, примусова депортація цивільного населення, знищення цивільної інфраструктури Маріуполя, Харкова, Чернігова, Кременчука, Херсона, Миколаєва, Нікополя, Львова інших населених пунктів, звірства в Ірпіні, Бучі, Гостомелі, Бородянці, Ізюмі, Куп'янську, окупація окремих регіонів країни, що дозволяє ставити питання про геноцид українського народу.

За статистичними даними Офісу Генерального прокурора станом на 26 березня 2023 р. в Україні зареєстровано 76 518 злочинів агресії та воєнних злочинів, 16 885 злочинів проти національної безпеки. За даними ювенальних прокурорів, 1 407 дітей постраждало в Україні внаслідок повномасштабної збройної агресії РФ. При цьому, 465 дітей загинуло та понад 942 отримали поранення різного ступеню тяжкості [2; 3]. За даними Офісу Генерального прокурора, за рік повномасштабної війни Росія

цілеспрямованими атаками зруйнувала або пошкодила понад 81 тисячу цивільних об'єктів: понад 62 тисячі житлових будинків, понад 450 медичних закладів [4]. Через масовані бомбардування та обстріли збройними силами РФ пошкоджено 3 126 закладів освіти, 438 з них зруйновано повністю [5]. Росія у XXI ст. руйнує критичну інфраструктуру, вбиває цивільне населення, депортує дітей, викрадає зерно, блокує українські порти, намагається вчинити світову продовольчу кризу.

Російські окупаційні війська лише упродовж тижня (з 27 жовтня по 3 листопада 2022 р.) запустили 68 ракет та застосували 30 дронів-камікадзе по об'єктах на території України. Масовані ракетні удари по енергетичних об'єктах України відбулися 15 листопада, коли було випущено понад 90 ракет та 10 дронів-камікадзе і через це близько 20 мільйонів людей залишилися без енергопостачання.

Відображення воєнних та інших злочинів міжнародного характеру віддзеркалюється у інформаційному просторі. Значна кількість інформації про вчинені міжнародні злочини зберігається в електронних джерелах, комп'ютерних системах, додатках до смартфонів, планшетів тощо. У цьому сенсі суттєвого значення набувають підходи щодо можливостей роботи з так званими цифровими доказами (цифровою інформацією або електронними слідами) – інформацією, яка створена за допомогою високих інформаційних технологій.

У наукових джерелах зарубіжних країн широкого застосування набув термін "digital evidences" (цифрові докази), під якими розуміють будь-які збережені дані або дані, що передаються з використанням комп'ютерної чи іншої техніки [6, с. 257]. Поряд із терміном «цифрові докази» використовуються й інші, наприклад: «електронні докази», «електронні сліди», «цифрові джерела інформації», «електронні документи» тощо. Цифрові докази вимагають новітніх підходів до їх збирання, зберігання, використання та дослідження під час доказування у кримінальному провадженні.

Важливим інноваційним напрямом у розвитку криміналістики та судової експертизи є використання цифрової інформації. Криміналістичні знання відображають певні тенденції глобалізованого світу. Фактично можна констатувати появу окремого криміналістичного напрямку – «цифрової криміналістики».

Цифрова криміналістика (Digital Forensics) – окрема криміналістична теорія та вид судової експертизи, що ставить своїм завданням дослідження цифрових доказів з використанням криміналістичної техніки та наявних методик в цілях досудового розслідування та судового розгляду [7, с. 129–130]. Цифрова криміналістика має відношення до процесу збирання, отримання, збереження, аналізу та подання електронних (цифрових) доказів у досудовому та судовому провадженні.

Розвиток цифрової криміналістики відбувається у трьох основних напрямах: 1) формування окремої наукової галузі в криміналістиці; 2) застосування спеціальних знань під час роботи з цифровими доказами; 3) проведення судових експертиз (зокрема, комп'ютерно-технічної експертизи).

Офіс Генерального прокурора разом з українськими та міжнародними партнерами створив спеціальний ресурс ***Warcrimes*** з метою документування воєнних злочинів та злочинів проти людяності, вчинених під час повномасштабної війни в Україні. Задокументовані докази будуть використані для кримінального переслідування осіб причетних до злочинів відповідно до українського законодавства, а також у Міжнародному кримінальному суді та в спеціальному трибуналі після його створення [8]. На сайті Офісу Генерального прокурора запропоновано алгоритм дій для потерпілих та свідків щодо фіксації воєнних злочинів з можливістю надіслати відео- та фотоматеріали, які підтверджують вчинення злочинів.

Важливу роль у збиранні даних про факти вчинення злочину агресії, злочину геноциду, злочинів проти людяності, воєнних злочинів мають здійснювати не лише органи правопорядку, а й неурядові, громадські організації. Суттєвою може бути допомога таких організацій у документуванні (фіксації) воєнних злочинів. Ця допомога може стати критично важливою не лише для початку досудового розслідування в Україні, а й для надання необхідних показань (даних) для роботи міжнародних судів (перш за все, Міжнародного кримінального суду). Прикладом такої діяльності є коаліція «Україна. 5 ранку», яку утворили 16 українських правозахисних організації саме для фіксації воєнних злочинів, злочинів проти людяності, інших грубих порушень прав людини. Аналогічні функції для фіксації закордоном воєнних злочинів, вчинених в Україні (інформація, яка прийма-

ється від біженців та тимчасово переміщених осіб) взяв на себе проект «Соняшники» [9, с. 259].

Постає питання про необхідність розроблення певних алгоритмів, правил, опитувальників щодо збирання, документування та фіксації доказової інформації. Можливо говорити й про необхідність розроблення криміналістичних методик розслідування міжнародних злочинів, формування системи наукових положень і рекомендацій щодо організації та здійснення розслідування та запобігання окремим видам злочинів (розроблення типових систем (алгоритмів) дій уповноважених осіб).

У цьому відношенні важливого значення набувають положення «Протоколу Берклі» (The Berkeley Protocol on Digital Open Source Investigations) [10], які містять поради щодо фіксації цифрових доказів (цифрової інформації). Протокол Берклі – є посібником з ефективного використання цифрової інформації з відкритим вихідним кодом при розслідуванні порушень міжнародного кримінального права, права людини та гуманітарного права [11].

Протокол Берклі – рекомендаційний документ, який у 2020 р. представили Центр прав людини Університету Берклі в Каліфорнії та Офіс Верховного комісара ООН з прав людини. Він окреслює мінімальні стандарти для пошуку, збирання, зберігання, перевірки та аналізу відкритих джерел, і може слугувати практичним посібником для юристів (адвокатів), журналістів, правоохоронних органів та дослідників. Закріплені стандарти є основою будь-якого OSINT-проєкту, тобто розвідки на основі відкритих джерел [12].

У Протоколі Берклі вказано, що «розслідування з використанням відкритих даних – це розслідування, яке повністю або частково спираються на загальнодоступну інформацію для проведення офіційних та систематичних онлайн-розслідувань щодо передбачуваних правопорушень… Інформація у відкритому доступі може надавати підказки, підтримувати результати розвідки та служити прямим доказом у судах» [13]. До джерел у відкритому доступі віднесено: a) фотографії, відео, інші публікації; b) контент створений користувачем у соціальних мережах, таких як You Tube, Facebook, Instagram та ін.; c) дані супутникових знімків [14].

Література

1. The UN Refugee Agency. URL: https://www.unhcr.org/ua/contact-us-ua.

2. Офіс Генерального прокурора. URL: https://www.gp.gov.ua.

3. Офіс Генерального прокурора. URL: https://m.facebook.com/1000064585280174.

4. В Україні вже зафіксували понад 71 тисячу воєнних злочинів РФ. URL: https://www.ukrinform.ua/amp/rubric-society/3682265-v-ukraine-vze-zafiksuvali-ponad-71tisacu-voennih-zlociniv-rf.html.

5. Офіс Генерального прокурора. URL: https://m.facebook.com/1000064585280174.

6. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету.* Сер.: Юриспруденція. 2013. № 5. С. 257.

7. Шепітько В., Шепітько М. Кримінальне право, криміналістика та судові науки: енциклопелія. Харків: Право, 2021. С. 129–130.

8. Офіс Генерального прокурора. URL: https://warcrimes.gov.ua.

9. Шепітько М. В. Про роль неурядових організацій в протидії кримінальним правопорушенням в умовах війни. *Матеріали VIII (XXI) Львівського форуму кримінальної юстиції: Українська кримінальна юстиція в умовах війни* (Львів, 9 червня 2022). Львів: ЛьвДУВС. 2022. С. 259.

10. ООН. Права человека. Управление Верховного Комиссара. *Протокол Беркли по ведению расследований с использованием открытых цифровых данных. Практическое руководство по эффективному использованию открытых цифровых данных при расследовании нарушений международного* уголовного права прав человека и международного гуманитарного права. URL: https://www.ohchr.org/ru/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source.

11. GRACERS. Law Firm. *Протокол Берклі - принцип ведення розслідування з використанням електронних* цифрових даних. URL: https://gracers.com/pres-centr/protocol-berkli-princip-vedennya-rozsliduvannya/.

12. Центр демократії та верховенства права. Протокл Берклі: як відкриті джерела допомогають притягнути Росію до відповідальності. URL: https://cedem.org.ua/news/protocol-berkli.

13. Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf.

14. Асоціація жінок-юристок України. *Протокол Берклі щодо розслідування із використанням відкритих цифрових даних.* URL: https://jurfem.com.ua/protocol-berkli-schodo-rozsliduvannia-iz-vykorystannyam-zyfrovych-danych/.

Хороновський О. І.
кандидат юридичних наук,
Національна академія СБ України

ДЕТЕРМІНАЦІЯ ЗАГРОЗ ЕКОНОМІЧНІЙ БЕЗПЕЦІ ДЕРЖАВИ, ПОВ'ЯЗАНИХ З ДІЯЛЬНОСТЮ ТРАНСНАЦІОНАЛЬНИХ ОРГАНІЗОВАНИХ ЗЛОЧИННИХ УГРУПУВАНЬ

Для України транснаціональна організована злочинність становить реальні загрози економічній безпеці, оскільки сучасний стан економіки, участь у міжнародному економічному та фінансовому співробітництві, стан правоохоронної системи та державних інститутів створює сприятливе середовище для її розвитку.

Розгляд даного питання розпочнемо із з'ясування змісту поняття «загрози економічній безпеці держави». В Законі України «Про національну безпеку України» знаходимо наступне визначення загроз в контексті забезпечення національної безпеки – явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України [1].

В Указі Президента України «Про стратегію національної безпеки України» від 14.09.2020 № 392/2020 (далі – Указ) визначено поточні та прогнозовані загрози національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов [2]. Проаналізувавши положення Указу, до загроз суто економічній безпеці держави в контексті протидії транснаціональній організованій злочинності нами віднесено наступні:

– сучасна модель глобалізації уможливила поширення міжнародної злочинності, зокрема у легалізації (відмивання) доходів, одержаних злочинним шляхом;

– непослідовність та незавершеність реформ і корупція перешкоджають виведенню української економіки з депресивного стану, унеможливлюють її стале і динамічне зростання, підвищують уразливість до загроз, підживлюють кримінальне середовище;

– недостатній захист права власності, повільний розвиток ринкових відносин у ключових сферах, у тому числі в користуванні землею і надрами, значна роль державного сектору в економіці, недосконаліть та фрагментарність законодавства стримують економічне зростання, залучення внутрішніх та зовнішніх інвестицій;

– недостатній рівень конкуренції та панування монополій, зокрема в енергетичній сфері та інфраструктурі, низька енергоефективність зменшують конкурентоспроможність України, загрожують добробуту її громадян.

Слід зазначити, що будь-яка із поточних та прогнозованих загроз, визначених Указом, може мати прямий чи опосередкований вплив на сферу економічної безпеки, та за своєю природою вважатися її загрозою. В той же час, у даному контексті ми виходили із суто економічних категорій та їх безпосереднього відношення до функціонування національної економіки.

На нашу думку, недоліком чинного законодавства є те, що загрози економічній безпеці розглядаються лише в рамках національної безпеки, при цьому загрози економічній безпеці держави не систематизовано за окремими складовими економічної безпеки держави, що визначені Методичними рекомендаціями щодо розрахунку рівня економічної безпеки України (наказ Мінекономрозвитку України від 29.10.2013 р. № 1277) [3]. До того ж у зазначених вище нормативно-правових актах, а також у Концепції забезпечення національної безпеки у фінансовій сфері, схваленій розпорядженням Кабінету Міністрів України від 15.08.2012 р. № 569-р [4], визначені загрози лише у деяких сферах економічної безпеки держави, а загрози економічній безпеці держави у решті її складових на законодавчому рівні не декларуються й фактично ігноруються.

Вважаємо, що окремо мають бути виділені загрози фінансовій безпеці як основної складової економічної безпеки, які в сучасних умовах мають максимальний рівень впливу та потребують розробки заходів з їх ліквідації у рамках реформування фінансової системи держави. Водночас, однією з таких загроз фінансовій безпеці повинна бути діяльність транснаціональних організованих злочинних угрупувань на шкоду економічним інтересам держави.

Чинне законодавство не класифікує загрози національній безпеці ні за критеріями, ні за сферами. В той же час, у науковій

літературі запропоновано різні критерії класифікації загроз економічній безпеці.

Найбільш поширеним у науковій літературі є поділ загроз економічній безпеці держави за місцем їх виникнення на внутрішні та зовнішні [5].

З точки зору сучасних концепцій забезпечення економічної безпеки держави особливої уваги також набуває класифікація загроз на реальні та потенційні [6].

В системі забезпечення економічної безпеки держави також важливою є класифікація загроз за масштабами їх реалізації, під якими розуміється просторовий розмах негативних чинників безпеки, наявність яких перешкоджає реалізації економічних інтересів держави. За масштабом загрози пропонується поділяти на загальнонаціональні, які стосуються всіх суб'єктів економічної безпеки держави та проявляються на загальнонаціональному рівні, локальні, що проявляються за окремими складовими економічної безпеки й зачіпають національні економічні інтереси певних груп суб'єктів економічної безпеки, та індивідуальні, які перешкоджають реалізації національних економічних інтересів окремих суб'єктів економічної безпеки [7].

Що стосується предмета нашого дослідження, ми класифікуємо загрози економічній безпеці держави за проявом джерела загрози, до якого відносимо діяльність транснаціональних організованих злочинних угрупувань на шкоду економічним інтересам держави.

Щодо транснаціональної організованої злочинності на шкоду економічним інтересам держави, у вітчизняній кримінології традиційним є уявлення, що її корені сягають радянських часів, коли у 60-80 роки несприятлива економічна ситуація потягла негативні кількісні і якісні зміни в злочинності. Зросла питома вага злочинів у сфері економіки, матеріальні збитки від них збільшились у багато разів. У зв'язку з послабленням контролю правоохоронних органів почало відбуватися зрощення крупних розкрадачів соціалістичної власності, тіньових ділків-підприємців (цеховиків) з корумпованими представниками партійного та державного апаратів, і усі вони отримали можливість злочинним шляхом отримувати надприбутки. Фактично в останні десятиліття радянської системи був створений потужний прошарок економічного криміналітету, що суттєво зріс та збагатився в період перебудови та перерозподілу власності [8, с. 8].

Надалі, в кінці 80-х – на початку 90-х років відбувся процес спочатку протистояння, а потім – зрощування ділків тіньової економіки зі злочинними угрупованнями спочатку традиційної загальнокримінальної спрямованості. Активна консолідація злочинних угруповань поступово тягла за собою встановлення ними контролю за цілими галузями торгівлі, виробництва, транспорту, малого, середнього і великого підприємництва, фінансовими операціями.

Починаючи з 90-х років поширенню негативних процесів сприяли такі чинники, як недосконалість вітчизняної законодавчої бази, що регулювала відносини у сфері економіки та державного управління, велика кількість безробітних і малозабезпечених верств населення, які ставали потенційним резервом кадрів для різноманітних злочинних (у тому числі організованих) угруповань.

Поступово, наприкінці першої половини 90-х років почали складатися організовані злочинні угруповання на основі своєрідного союзу представників адміністративно-господарської номенклатури, ділків від економіки і криміналітету. Згодом цей союз набув постійного та системного характеру [8, с. 9].

З часом організовані злочинні угруповання вийшли далеко за межі території держави, встановлюючи зв’язки як з кримінальними структурами, так і з законно діючими економічними суб’єктами. Зміцнювалась їх матеріально-технічна і фінансова база, зростав професіоналізм, організованість і взаємодія з аналогічними структурами за кордоном. Поширенню транснаціональних зв’язків організованих злочинних угруповань сприяло і серединне географічне розташування України, найбільша в Європі довжина кордонів (8215 км), що у поєднанні зі складними соціальноекономічними процесами як у нашій країні, так і у сусідніх державах, призвело до потрапляння країни в один з епіцентрів транснаціональних злочинних потоків.

В цілому ж, на нашу думку, до середини 2000-х років діяльність транснаціональних організованих злочинних угруповань на шкоду економічним інтересам держави набула сучасного вигляду, охопивши такі сфери економіки як: кредитно-фінансова, банківська, приватизації, нерухомості, фондового ринку, віртуальних активів, зовнішньоекономічної діяльності та інші.

Вагомими дестабілізуючими чинниками в Україні, пов'язаними з діяннями транснаціональних злочинних угрупувань, є: криміналізація сфери економічних відносин (оборудки на каналі зовнішніх інвестицій та кредитів, спроби встановити контроль над прибутковими суб'єктами господарської діяльності, транспорту та зв'язку); протиправні операції з фінансовими ресурсами (шахрайство, переведення коштів за межі України з використанням; легалізація, відмивання доходів від злочинної діяльності); шахрайство із застосуванням наднових платіжних засобів та комп'ютерів тощо [9].

Існує думка, що основну загрозу національній безпеці в економічній сфері транснаціональна організована злочинність становить через використання інструментів легалізації доходів, одержаних злочинним шляхом. Вплив на економічну сферу проявляється як шляхом встановлення контролю над секторами економіки та окремими суб'єктами підприємництва, так і через легалізацію доходів, одержаних злочинним шляхом, що є невід'ємною складовою системи організованої злочинності, має виражений транснаціональний характер. Легалізація доходів, одержаних злочинним шляхом, є ланкою, що з'єднує кримінальний сектор тіньової економіки та легальну економіку каналом, через який доходи, отримані від злочинної діяльності, надходять до законної сфери економічних відносин. У контексті протидії транснаціональній організованій злочинності легалізацію доходів, одержаних злочинним шляхом, слід розглядати як форму організованої злочинної діяльності, що полягає в інвестуванні коштів, одержаних злочинним шляхом, в легальний сектор економіки [10]. Вважаємо, що такий підхід до визначення загроз економічній безпеці держави, обумовлених діяльністю транснаціональних організованих злочинних угрупувань є дещо поверхневим та не розкриває у повній мірі їх сутності та змісту. Легалізація доходів, одержаних злочинним шляхом є однією із форм злочинної діяльності транснаціональних організованих злочинних угрупувань, яка присутня в діяльності абсолютно всіх злочинних елементів з корисливою мотивацією. Тому визначення легалізації доходів, одержаних злочинним шляхом як загрози економічній безпеці держави у даному контексті є надто абстрактним.

Отже, з урахуванням вищевикладеного до основних загроз економічній безпеці держави, пов'язаних з діяльністю транснаціональних організованих злочинних угрупувань можемо віднести:

– запровадження та реалізація протиправних схем та механізмів, зокрема в ході приватизації, публічних закупівель, управління державними корпоративними правами, банкрутства державних підприємств, адміністрування ПДВ та ін.;

– корупційні зв'язки в органах державної влади та місцевого самоврядування, які дозволяють приймати економічно-вигідні рішення на користь криміналітету всупереч економічним інтересам держави;

– використання міжнародних та внутрішньодержавних платіжних систем для перерахування злочинних активів у будь-які частини світу;

– отримання переваг у сфері публічних закупівель, державних пільг та інших економічно необґрунтованих преференцій;

– заволодіння українськими об'єктами інтелектуальної власності, відомостями, що містять комерційну таємницю та їх використання у протиправній діяльності;

– отримання та використання інформації з обмеженим доступом у сфері економіки, яка циркулює на об'єктах критичної інфраструктури в злочинних цілях;

– лобіювання прийняття нормативно-правових актів у власних цілях всупереч економічним інтересам держави;

– переміщення капіталів за кордон з метою ухилення від оподаткування та легалізації злочинних прибутків в сприятливих юрисдикціях;

– зниження інвестиційної привабливості держави та відсутність здорової конкуренції в національній економіці в силу застосування «нечесних» правил бізнесу;

– стримання розвитку ринкових відносин у ключових сферах, недопущення удосконалення законодавства в економічній сфері.

Запропоновані нами загрози економічній безпеці держави, пов'язані з діяльністю транснаціональних організованих злочинних угрупувань не є вичерпними, залежать від багатьох суб'єктивних та об'єктивних факторів, еволюціонують та деградують в силу зміни суспільних відносин.

Література

1. Про національну безпеку : Закон України від 21.06.2018 № 2469. URL: https://zakon.rada.gov.ua/laws/show/2469-19#n355 (дата звернення 01.09.2021).

2. Про стратегію національної безпеки України : Указ Президента України від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення 01.09.2021).

3. Про затвердження Методичних рекомендацій щодо розрахунку рівня економічної безпеки України : Наказ Міністерства економічного розвитку і торгівлі України від 29.10.2013 № 1277. URL: https://zakon.rada.gov.ua/rada/show/v1277731-13#Text (дата звернення 01.09.2021).

4. Про схвалення Концепції забезпечення національної безпеки у фінансовій сфері : Розпорядження Кабінету Міністрів України від 15.08.2012 № 569-р. URL: https://zakon.rada.gov.ua.laws.show/569-2012 (дата звернення 01.09.2021)

5. Пастернак-Таранушенко Г. А. Економічна безпека держави. Статика процесу забезпечення. Київ : Кондор, 2002. 302 с.

6. Пироженко В. Методологія операціоналізації основних понять національної безпеки : гуманітарна складова. *Політичний менеджмент*. 2006. № 3. С. 21–34.

7. Коломієць І. Ф., Пабат О. В. Загрози та виклики економічній безпеці держави : синергетичний аспект. *Економіка*. 2011. № 1. С. 7-12.

8. Корнієнко М. В. Організована злочинність в Україні: сучасний стан, кримінологічна характеристика, заходи протидії. Київ : Фонд Юрнауки, 2004. 300 с.

9. Вербенський М. Г. Транснаціональна злочинність : кримінологічна характеристика та шляхи запобігання: дис. ... д-ра юрид. наук : 12.00.08. Дніпропетровськ, 2010. 503 с.

10. Новікова Л. В. Глобалізація та транснаціональна економічна злочинність: питання сьогодення. Право і безпека. 2010. № 3. С. 26-30.

Орел О. В.
кандидат юридичних наук, доцент,
Національна академія Національної гвардії України
(м. Харків)
Мідіна А. С.
Харківський національний університет ім. В. Н. Каразіна

OSINT ЯК КЛЮЧ ДО НОВИХ МОЖЛИВОСТЕЙ У ПРАВОВОМУ ПОЛІ ПІД ЧАС ВІЙНИ

Конституція України, будучи Основним законом нашої держави, містить положення (ч. 3 ст. 17), в яких зазначено, що забезпечення державної безпеки і захист державного кордону

України покладається на відповідні військові формування та правоохоронні органи держави, організація і порядок діяльності яких визначаються законом [1].

Так, Національна гвардія України, будучи учасником правовідносин у сфері протидії загрозам національній безпеці України, здійснює діяльність врегульовану нормами військово-адміністративного права, що ґрунтується та змінюється у залежності від адміністративно-правових режимів; має визначені законом повноваження щодо виявлення, відвернення, знищення та зменшення негативного впливу з боку агресора. Приймаючи активну участь в обороні держави, здійснюючи протидію агресору, НГУ сприяє збереженню та захисту національної державності.

24 лютого 2022 року в наслідок збройної агресії з боку Російської Федерації на території України був введений правовий режим воєнного стану, який створив низку особливостей та проблем, які притаманні саме цьому періоду, це: блокування інтернет-ресурсів, надлишкове втручання політики держави, надлишкове маніпулювання мисленням та поведінкою населення шляхом засобів масової інформації, пропагандою тощо; у правовому полі – розпорошеність відповідних норм права у чисельних нормативно-правових актах; низький рівень правової реалізації; наявність чисельних бланкетних чи відсильних норм права, понять, базових дефініцій – призвели до ряду нових злочинів і правопорушень. При цьому, постійне підтримання та підвищення бойового потенціалу, створення ефективного, комплексного та багатофункціонального державного інструментарію для забезпечення національної безпеки нашої країни сьогодні посідає пріоритетне місце, що дає підґрунтя для широкої академічної дискусії й пошуків найбільш виваженого і збалансованого бачення майбутнього нашої держави.

Ми знаходимося в світі, що не стоїть на місті, а постійно розвивається та видозмінюється. Гібридні прояви війни, нестабільність держави та уряду – це плацдарм для протиправних діянь і злочинці успішно використовують кожну нішу, яка слабо контролюється, шукають все нові можливості для створення спектру загроз національній безпеці України. Вони сьогодні мають повну вищу освіту, прагнуть до просування по соціальних і службових сходах, є схильними до лідерства. Використо-

вуючи сучасні технології, постійно підвищують свій рівень кваліфікації, а наявність війни їм в цьому допомагає.

Пошуковик OSINT – є ключем до нових можливостей для сектору безпеки і оборони, особливо під час війни. Він допомагає не тільки зібрати, перевірити, проаналізувати інформацію про потенційних злочинців (події, явища, підприємства, установи, організації тощо), але й автоматизувати робоче місце кожного представника сектору безпеки і оборони. Оскільки допомагає в отриманні доказової бази, знаходженні потенційних ризиків та визначенні оцінки захищеності відповідних процесів і явищ, мінімізуванні трудової активності військовослужбовця та підвищенні рівня збереження його здоров'я, прийнятті управлінських рішень.

Головна перевага OSINT як у мирний, так і воєнний час – це його використання без знань мови програмування; недолік – визначені обмеження при застосуванні у державній, військовій та правоохоронній сферах. Саме з цієї причини для технологій OSINT створено найбільшу кількість методик, технік і технологій [2-5]. Джерелами цього структурованого підходу є: засоби масової інформації, мережа Інтернет, публічні урядові (державні) дані, академічні публікації, дані комерційного характеру тощо.

Як відомо, для правознавця достатньо пасивного інструментарію OSINT, однак для підвищення його власного професійного рівня, спроможності прогнозувати визначені явища та наслідки, що підтверджують особисту інтуїцію, було б доцільно володіти активним інструментарієм OSINT. Те ж саме стосується керівників різної ланки для отримання характеризуючих даних щодо підлеглої особи.

Висока деталізація даної платформи дозволяє представнику сектору безпеки і оборони в цілому та правознавцю зокрема, ефективніше використовувати час, якого у нього завжди в обмаль, а також більш критично сприймати отриману в ході розслідування інформацію. Крім цього, здобуті дані дають поштовх до нових потреб в отриманні інформації та пошуків їх задоволення. А це рішучі кроки вперед, кроки до майбутньої перемоги, кроки до нових зрушень у нашій спільній роботі.

Література

1. Конституція України : Закон України від 28.06.1996 // Відомості Верховної Ради України. 1996. № 30. Ст. 141.

2. Army techniques publication FMI 2-22.9. Headquarters Department of the Army Washington, DC, 7 2012.

3. Dmytro Lande, Ellina Shnurko-Tabakova. OSINT as a part of cyber defense system. *Theoretical and Applied Cybersecurity*, 2019. № 1. P. 103-108. OSINT Academy. Режим доступу: URL: https://www.youtube.com/playlist?list=PL-9OTQQwXf2XuDGO_EIewUOpzUXLDDfcL

4. Steele, R.D. Open Source Intelligence: READER Proceedings, 1997 Volume II 6th International Conference & Exhibit Global Security & Global Comp, 1997. P. 329-341.

5. Берд К. Модель OSINT. *Компьютерра.* 2007. № 22.

Кудрявцева Н. О.
Національна академія СБ України

ІДЕЯ СТРУКТУРИЗАЦІЇ КОНТЕНТУ ДЛЯ СПРОЩЕННЯ ПОШУКУ ІНФОРМАЦІЇ У WEB-СЕРЕДОВИЩІ

З кожним днем все більш актуальним і важливим в сучасному світі стає процес адаптації громадян до цифрового суспільства. І якщо нещодавно ми тільки почали прилаштовуватися до належного здійснення реальних взаємовідносин, дотримання правил й законодавчих норм, то сьогодні уже віртуальний простір почав змінювати спосіб життя та роботи, став невід'ємною частиною життя людей і без належної попередньої адаптації до змін вимагає нових негайних пристосувань. Оскільки технології стають все більш розповсюдженими в нашому житті, важливо розвивати навички, необхідні для успішного функціонування людини в цифровому середовищі. Це насамперед навички пошуку інформації в Інтернеті, електронної комунікації, навички кібербезпеки та уникнення шахрайства тощо.

На відміну від традиційного освіту, особливостями цифрової реальності є те, що в цифровому світі фізичний контакт між людьми й предметами реального світу відсутній, обсяг інформаційного потоку надзвичайно масивний, що впливає на зниження критичності її сприйняття, існує висока імовірність виникнення непорозумінь та конфліктів через відсутність невербальної комунікації та контексту. Також в Інтернеті може виникати більш висока ймовірність порушення приватності та безпеки, оскільки він є публічним простором, а деякі користувачі можуть бути анонімними. Крім того, за допомогою використан-

ня Інтернету стало зручніше здійснювати фінансові операції, проведення яких теж збільшує ризик шахрайства та крадіжки особистої інформації он-лайн. Більше того, Інтернет-технології дозволяють людям взаємодіяти та отримувати будь-яку інформацію без прив'язки до часу доби та місця перебування, забезпечуючи при цьому високу мобільність та одночасне відвідування різних заходів. Як підсумок, Інтернет-реальність становить собою великий масив неконтрольованої інформації, що постійно подається та безперервно оновлюється й модернізується для огляду громадськості.

На перший погляд, цифрове суспільство характеризується певними правилами за допомогою використання яких кваліфіковані спеціалісти можуть простежити «пошуковий шлях чи слід» користувача. Водночас, коли мова йде про інформацію, що там подається, то правила відсутні і відстежити її рух, фільтрувати достовірність чи встановити реальне авторство стає уже значно важче. У реальності ж ми можемо бачити співрозмовника, отримуємо від нього інформацію та даємо оцінку з огляду на особливості невербальної поведінки співбесідника (жести, поведінка, емоції, зовнішній вигляд, вік, статус, соціальна роль тощо). Загальновідомим фактом є те, що понад 80-90 відсотків інформації передається немовленнєвим шляхом, інші 20-10 відсотків за допомогою слів. Виходить, що в онлайн-реальності додаткову інформацію ми додумуємо самі (виходячи із сервісів розміщення на них повідомлення, із часу, з контексту поданої інформації). Таким чином, незважаючи на свою пасивність, Інтернет-контент дає можливість володіти значно меншою частиною достовірної інформації, ніж це на перший погляд здається. Також ми маємо великий потік неконтрольованої інформації, що щодня дублюється і поширюється, проте володіємо обмеженими ресурсами у здійсненні контролю за її поширенням та протидії дезінформації.

Для уникнення цього варто вжити заходів щодо максимального наближення віртуального світу до правил існування реальності. Для прикладу, у звичайному житті є можливість персональної ідентифікації, під час реального спілкування ми візуально можемо встановити особу (як вона себе представляє, за потреби маємо можливість з'ясувати її офіційне ім'я та підтвердити його) і визначити статус співрозмовника. За аналогією в Інтернет мережі слід заборонити вхід та користування під неві-

домими іменами (а якщо й здійснювати, то обмежити можливість реєстрації у системі лише під одним іменем), а зміну імені в системі здійснювати за встановленими правилами.

Також важливо встановити загальнодоступний механізм ідентифікації статусу фізичної особи. Так, для прикладу, система повинна пропонувати можливість публікації статей, особистих думок, записів чи коментарів під обліковими записами «посадової особи державного органу», «представника громадської організації», «представника засобу масової інформації» чи «окремого громадянина» тощо. Водночас рекомендовано, щоб статус публікації особи позначався маркуванням поряд з іменем Інтернет-користувача і був відкритим не лише для спеціалістів з Інтернет-технологій, але й для інших користувачів web-середовища.

Безумовно, що запропоновані кроки можуть піддаватися широкому дискутуванню і поки що розглядаються виключно як початкові ідеї, втілення яких може стати вагомим засобом у сфері боротьби з дезінформацією, а також допоможе знизити кількість правопорушень в мережі Інтернет і дозволить ефективно здійснювати зацікавленими користувачами заходи з пошуку та аналізу потрібної інформації в мережі Інтернет.

Галустян О. А.
кандидат юридичних наук,
Національна академія внутрішніх справ

ПРОФАЙЛІНГ ТА OSINT: СУЧАСНІ ТЕХНОЛОГІЇ ВИЯВЛЕННЯ КОЛАБОРАНТІВ ТА КОЛАБОРАЦІЙНОЇ ДІЯЛЬНОСТІ В УМОВАХ ВОЄННОГО ЧАСУ

У зв’язку з військовою агресією російської федерації проти України Указом Президента України від 24 лютого 2022 року № 64/2022 «Про введення воєнного стану в Україні», затвердженим Законом України від 24 лютого 2022 року № 2102-IX, в Україні введено воєнний стан [1; 3].

15 березня 2022 року набрав чинності Закон України від 03.03.2022 № 2108-IX «Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колаборацію діяльність», який спрямований на вре-

гулювання одного з найважливіших питань, яке наразі гостро постало перед Україною – питання заборони колабораціонізму.

Колаборант – особа, яка усвідомлено співпрацює із окупаційною цивільною чи військовою владою на шкоду власній державі. Згідно з загальним національним правом діяльність колаборантів визнавалась як зрада громадян та як зрада інтересів своєї держави [2].

Визначення юридичного поняття колабораціонізму та відповідальність за цю діяльність передбачені статтею 111-1 КК України. Поряд з тим державна зрада – це умисні дії, вчинені громадянином України на шкоду суверенітету, територіальній цілісності, недоторканості, обороноздатності, державній, економічній чи інформаційній безпеці.

Так, колаборційною діяльністю визнається:

– публічне заперечення збройної агресії проти України, публічні заклики до співпраці з рф (у мережі Інтернет або за допомогою ЗМІ);

– зайняття посади у незаконних органах влади на тимчасово окупованій території, обрання до таких органів;

– пропаганда в закладах освіти;

– передача матеріальних ресурсів незаконним збройним формуванням на тимчасово окупованій території;

– організація та проведення виборів, референдумів на тимчасово окупованій території або публічні заклики до їх проведення;

– організація та проведення з'їздів, зборів, мітингів, демонстрацій, інформаційна співпраця з окупаційною владою;

– зайняття посади в незаконних судових або правоохоронних органах на тимчасово окупованій території;

– участь у незаконних збройних формуваннях держави-агресора;

– допомога у веденні бойових дій проти ЗСУ, добровольчих формувань, утворених для захисту України [3].

Серед перспективних інструментів виявлення колаборантів та колаборційної діяльності можна вважати профайлінг та розвідку з відкритих джерел (OSINT).

Під *профайлінгом* розуміють практику поліції, за якої певний набір характеристик (профілів) використовують для пошуку та затримання особи, яка вчинила злочин (кримінальний

профайлінг), чи для виявлення осіб, які, ймовірно, причетні до злочинної діяльності (поведінковий профайлінг) [4, с. 2].

Обидва напрями профайлінгу мають забезпечити високоефективний системний підхід щодо виявлення колаборантів і колабораційної діяльності в умовах воєнного часу.

Технології профайлінгу можна використовувати як в процесі безпосередньої міжособистісної взаємодії, так й опосередковано, шляхом вивчення інформації щодо будь якої людини.

Практика використання технологій профайлінгу дозволяє здійснити доволі точний аналіз та дійти обґрунтованих висновків щодо потенційної небезпеки окремого індивіда. Ця технологія на практиці підтвердила свою превентивну ефективність на об'єктах залізничного, автомобільного, водного та повітряного транспорту, а також у місцях масового скупчення людей та під час проведення масових заходів.

В кінці ХХ на початку ХХ1 сторіччя швидкісними темпами почали розвиватися інформаційні технології, Інтернет та соціальні мережі. Інтернет-простір є засобом формування специфічного різновиду комунікацій (Інтернет-комунікацій), які можливі в актуальному та мережевому режимах.

До жанрів електронної комунікації належать вебсайти, електронна пошта, чат, форум, блог, телеконференція, гостьова книга, дошка оголошень, електронний журнал, електронна бібліотека, домашня сторінка, каталог, рекламні банери тощо.

Інтернет-дискурс залежно від форми спілкування може бути різним за жанром: відеодискурс, чатдискурс, месенджердискурс (передбачають спілкування «тут і зараз», онлайн між адресатом і адресантом повідомлення), соціальні мережі, блоги (не завжди онлайн спілкування) [5, с. 24–25].

Особливу роль у використанні технологій профайлінгу з метою виявлення колаборантів та колабораційної діяльності має відігравати OSINT [6, с. 274].

OSINT (від англ. *open-source intelligence*) – це методи пошуку, збору, вибору та аналізу інформації, яка являє оперативний інтерес, з відкритих джерел [7].

До основних джерел online OSINT відносять: веб-сайти (Firefox, Chrome, Safari, Opera, Edge,Internet Explorer, Brave тощо); соціальні мережі (Facebook, Instagram, TikTok, LinkedIn, Twitter, Telegram тощо); особисті облікові дані (ім'я, прізвище, псевдонім, електронна адреса, номер телефону тощо); карти (усі

загальнодоступні джерела карт); документи (pdf, Docx тощо); фото/відеозображення; Ip-адреси; реєстри підприємств і державні реєстри; транзакції з віртуальними валютами (криптовалюти та їх блокчейни); Internet archives.

За допомогою OSINT у сучасному світі вирішуються різноманітні завдання на рівні держави, на кшталт, забезпечення національної безпеки або боротьби з тероризмом. Інструменти та технології OSINT дозволяють відстежувати погляди громадськості на різні теми, висвітлення з різних боків подій, що відбуваються у світі, отримувати потрібну інформацію, у тому числі щодо колаборантів та колабораційної діяльності в умовах широкомасштабного військового вторгнення рф в Україну та окупації частини її територій.

Профайлінг у контексті виявлення колаборантів та колабораційної діяльності передбачає сукупність заходів збору, аналізу та узагальнення інформації з метою складання психологічного портрету колаборанта та його затримання й притягнення до кримінальної відповідальності.

Використання циклу OSINT дозволяє раціоналізувати розвідувальні ресурси, спрямовуючи зусилля на пошук лише тієї інформації, яка не може бути знайдена у відкритих ресурсах. Адже використання OSINT актуально на початковому етапі виявлення колаборантів та колабораційної діяльності, оскільки попередній збір та аналіз інформації про особистість потенційного колаборанта дозволить визначити ключові моменти, які потребуватимуть поглибленої перевірки в ході профайлінгових дій.

Таким чином, комплексне використання технологій профайлінгу та OSINT має суттєвий потенціал, достатній для виявлення колаборантів та колабораційної діяльності в умовах воєнного часу.

Література

1. Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колабораційну діяльність: Закон України від 03.03.2022 р. № 2108-IX. URL: https://zakon.rada.gov.ua/laws/show/2108-20#Text.

2. Яке покарання чекає на колаборантів: роз'яснення суду. LIGA ZAKON. URL: https://jurliga.ligazakon.net/news/217118_yake-pokarannya-cheka-na-kolaborantv-rozyasnennya-sudu.

3. Кримінальна відповідальність за колабораційну діяльність: законодавчі зміни. Профспілка працівників освіти і науки України. Офіційний сайт. URL: https://pon.org.ua/novyny/9330-kryminalna-vidpovidalnist-za-kolaboraciinu-diialnist-zakonodavchi-zminy.html.

4. Галустян О.А., Захаренко Л.М., Мотлях О.І. Технології профайлінгу в слідчій діяльності. Київ: 2019. 45 с.

5. Галустян О.А., Захаренко Л.М., Казміренко В.О. Складання психологічного профілю невстановленої особи за характеристиками її письмового тексту (за заг. ред. О.І. Мотляха). Київ: 2020. 68 с.

6. Яровой Т.С. Перспективні інструменти нагляду за лобістською діяльністю: профайлінг та OSINT. Наукові перспективи № 5 (5). 2020. С. 269-277.

7. Уфімцева О.С. Використання OSINT в умовах збройної агресії рф проти України. URL: https://ua.softlist.com.ua/articles/top-10-luchshykh-ynstrumentov-osint-dlia-razvedki-s-otkrytym-ishodnym-kodom/.

Кіреєва О. С.
кандидат психологічних наук, доцент,
Національна академія
Державної прикордонної служби України

ВИКОРИСТАННЯ МЕТОДІВ OSINT В РОБОТІ КРИМІНАЛЬНИХ АНАЛІТИКІВ

В сьогоднішньому суспільстві відбувається глобальна інформатизація всіх сфер життя. Так, на сьогодні майже немає такої людини, яка б не користувалася соціальними мережами. З одного боку розвиток інформаційного суспільства має ряд позитивних зрушень: зростає ефективність праці, розвиток високих технологій, розширення меж спілкування тощо.

Однак, з іншого боку, багато злочинів, які відбуваються у сучасному світі, плануються саме в інтернет-просторі, використовуючи спілкування в месенджерах, надсилання фото з зашифрованим місцем злочину тощо.

З огляду на те, що на території України зараз відбуваються воєнні дії, спецслужби країни-агресора можуть використовувати соціальні мережі як для коригування вогню ворога, так і для проведення інформаційної війни. Тому, з початком повномасштабного вторгнення рф, громадян України неодноразово закликали не публікувати в соціальних мережах наслідки обстрілів,

не передавати жодну інформацію стосовно розташування стратегічних об’єктів по месенджерах.

В своїй повсякденній діяльності кримінальний аналітик щоденно стикається з необхідністю пошуку інформації стосовно об’єктів, які потрапили до сфери зацікавленості, тому застосування сучасних інформаційних технологій дозволяє йому здійснювати обробку великих масивів інформації та отримувати інформацію з найрізноманітніших інформаційних ресурсів.

Одним із методів збирання оперативної інформації є використання розвідки з відкритих джерел. OSINT (Open Source INTelligence) – це збір, аналіз, обробка даних, які знаходяться у загальному доступі, але ці дані завжди специфічні, тобто зібрані та структуровані особливим способом, задля відповіді на конкретне питання. OSINT є продуктивною системою протидії злочинам, які відбуваються у кіберпросторі, треба лише правильно використовувати цей метод, враховуючи міжнародний досвід і в деяких випадках дає змогу запобігти вчиненню злочину [1].

Враховуючи те, що OSINT передбачає пошук інформації з відкритих джерел, тобто це загальнодоступна інформація, така діяльність є цілком законною. Основними джерелами OSINT є Інтернет (соціальні мережі, блоги, відеохостинги, форуми, месенджери), журнали, газети, ЗМІ, радіо, публічні матеріали державних структур, загальнодоступні спостереження, звіти, статті, доповіді, конференції та т.п.

На сьогодні можна окреслити наступний список найкращих безкоштовних інструментів OSINT:

Maltego – потужний інструмент для побудови та вивчення зв’язків між різними суб’єктами та об’єктами. Maltego використовується для аналізу взаємозв’язків між людьми, компаніями, сайтами та пошуку загальнодоступної інформації. Maltego дозволяє зібрати воєдино інформацію та надати агреговані дані у вигляді візуальної карти. Працює на Java, і її можна встановити у Windows, macOS та Linux.

theHarvester – інструмент для пошуку та збирання адрес електронної пошти, пошуку піддоменів, пошуку даних про співробітників компанії. Простий та безкоштовний інструмент OSINT на Python. Він був розроблений для збору інформації з різних джерел, таких як пошукові системи, бази даних Shodan, Hunter, Baidu і т.д. Може знаходити інформацію про домени, піддомени, IP-адреси, облікові записи електронної пошти, імена

співробітників та багато іншого. Дозволяє використовувати модулі з API, такі як bingapi, gitHub та інші.

Metagoofil – утиліта, яка дозволяє завантажити всі документи з цільового сайту та витягти з них метадані. Це безкоштовний збирач метаданих, написаний на Python. Його використовують з метою вилучення інформації з документів: pdf, doc, XLS, ppt, ODP та ods, які знаходяться на цільовій веб-сторінці або будь-якому іншому загальнодоступному сайті. Інструмент використовує Google для пошуку документів, після чого завантажує їх, витягує та аналізує метадані. Він може знайти конфіденційну інформацію, таку як імена користувачів, електронні листи і т.д. Він також може показати шлях до файлів, які можуть розкрити особисті дані, мережеві імена, загальні ресурси і багато іншого.

SpiderFoot – безкоштовний інструмент із відкритим вихідним кодом на Python для автоматизованої розвідки та збору інформації щодо заданої мети. Інструмент може автоматично надсилати запити більш ніж у 100 загальнодоступних джерел і збирати інформацію про IP-адреси, домени, веб-сервери, адреси електронної пошти та багато іншого. Після вибору модулів SpiderFoot автоматично почне збирати інформацію та підготує детальний звіт. SpiderFoot доступний для Windows та Linux.

Framework - потужний та безкоштовний онлайн-сервіс, для пошуку різноманітної інформації. Він надає інформацію у вигляді інтерактивної інтелект-карти на базі Інтернету, яка візуально впорядковує інформацію. Framework популярний серед пентестерів. За допомогою цієї платформи можна переглядати різні інструменти OSINT, які фільтруються за категоріями. Наприклад, деякі категорії - це ім’я користувача, адреса електронної пошти, геолокація / карти, темна мережа, пошукові системи, транспорт, загальнодоступні записи та багато іншого [2].

DarkOwl Vision – пошук інформації у даркнеті Платформа дозволяє проводити моніторинг та аналітику загроз у просторі Dark web для ефективного пошуку скомпрометованих конфіденційних даних. Програма DarkOwl Vision в автоматичному режимі безперервно та анонімно займається збором, індексацією та ранжуванням важливих даних розвідки даркнету. Інтерфейс користувача зручний для роботи, пошукова система підтримує логічні вирази і фільтри.

PhoneInfoga – інструмент OSINT для пошуку за номером телефону. Це потужна програма, що дозволяє аналізувати телефонні номери та збирати потрібну інформацію. На першому етапі відбувається збір стандартних даних (країна, оператор, тип лінії). Після цього в пошукових системах фахівці знаходять слід, за яким можна визначити власника [3].

Важливою частиною побудови ефективної стратегії OSINT є пошук правильних інструментів. Об'єм та складність даних із відкритих джерел роблять ручну обробку даних неефективним рішенням для OSINT. Розуміння цих типів інструментів, варіантів та підходів дозволить підібрати правильний інструмент відповідно до заданих цілей розслідування.

Будь-яке розслідування складається з кількох етапів, включаючи збирання, обробку, аналіз та поширення інформації. Деякі інструменти призначені для допомоги на одному етапі, інші охоплюють процес розслідування. Немає єдиного способу класифікувати різні інструменти OSINT. Вибрані інструменти безпосередньо впливають на типи розслідувань, які можна ефективно проводити. Важливо враховувати функції та програми, що відповідають потребам, а також ключові переваги. Чим менше інструментів необхідно використовувати, тим простіше організувати розслідування, тим менше зусиль для цього потрібно. Крім того, єдина платформа знижує необхідність додаткової інтеграції даних, що в кінцевому підсумку може призвести до економії коштів.

Таким чином, узагальнюючи вищевикладене, можна виокремити чотири послідовні кроки для отримання інформації з Інтернет-ресурсів:

1. Складання плану пошуку. Для складання плану пошуку кримінальні аналітики повинні зрозуміти інформаційно-розвідувальні вимоги, які допоможуть визначити види необхідної інформації, місця їх пошуку, а також ключові слова, що використовуються при здійсненні пошуку. Після визначення спрямованості і ключових слів, кримінальні аналітики використовують інтернет-браузери і пошукові систем для підключення до раніше виявленим сайтам.

2. Проведення пошуку. З метою дослідження необхідного питання, кримінальні аналітики за допомогою відповідних запитів проводять первинний пошук ймовірних джерел інформації. Початковий пошук є першим з усіх наступних пошуків да-

них та інформації, які отримані і зареєстровані відповідно до плану дослідження. Отримана інформація автоматично інтегрується в відповідні цифрові або аналогові бази даних. Кримінальні аналітики повинні уникати спокуси використовувати тільки одну пошукову систему, оскільки кожна має свої сильні і слабкі сторони. Організаційні стандарти, досвід досліджень і експертні рекомендацій, зазвичай підказують яку пошукову систему необхідно використовувати.

3. Удосконалення техніки пошуку. Перші кілька сторінок результатів пошуку, як правило, є найбільш актуальними. Ґрунтуючись на цих сторінках, кримінальні аналітики аналізують перші результати пошуку на предмет важливості та точності, з метою визначення їх відповідності розвідувальним вимогам, а в разі необхідності відновлення пошуку. Результати первинного пошуку в Інтернеті можуть бути недостатні, щоб задовольнити інформаційно-розвідувальні вимоги. Кримінальні аналітики зазвичай використовують наступні методи поліпшення результатів пошуку: зміна порядку та критеріїв пошуку; зміна правопису і граматики; регулювання верхнього або нижнього регістру; використання інші варіанти ключових слів; пошук в результатах; пошук по колонках; пошук в кеш-пам’яті і архіві; укорочення URL; домени веб-сайтів.

4. Збереження (запис) результатів пошуку.

Так як основною метою OSINT є використання загальнодоступної інформації з відкритих джерел, не розкриваючи відомостей про своїх співробітників або організації, то процес використання загальнодоступної інформації з відкритих джерел, як правило, є анонімним і зменшує ризики потенційного розкриття.

Однак, під час проведенні досліджень в мережі інтернет і Deep Web існують неминучі загрози. Ведення розвідки в відкритих джерелах може поставити під загрозу безпеку операції і розкрити інформацію про користувача (кримінального аналітика) і через IP-адресу видати місце розташування його комп'ютерних систем.

Тому, під час здійснення пошуку інформації в мережі Інтернет, кримінальний аналітик повинен потурбуватися про інформаційну безпеку.

Отже ключовими факторами для успішного аналізу є: чітке розуміння цілей аналізу; неупередженість (максимальна об’єктивність аналітика); збір інформації з максимально мож-

ливої кількості відкритих джерел; застосування «коефіцієнтів ваги» до кожної інформації; чіткість представлення даних; грамотний аналіз отриманої інформації.

На теперішній час, у період воєнного стану в Україні, використання інструментів OSINT як ніколи раніше актуальне. Їх використання дозволить відфільтрувати фейкові новини, за допомогою пошуку по фото, тексту, джерелу. Методи OSINT надають можливість розкривати кримінальні злочини, визначати місця розташування техніки та живої сили ворога, фіксувати за супутниковими даними конкретні дії людей.

Література

1. Модель OSINT. Відкриті джерела у світі розвідки: веб-сайт : URL: http://strateger.net/model_osint_otkritie_istochniki_v_mire_razvedki (дата звернення 20.03.2023);

2. OSINT Інструменти для розслідування. URL : https://hackyourmom.com/kibervijna/ osint-akademiya/osint-instrumenty-dlya-rozsliduvannya/HackYourMom (дата звернення 20.03.2023);

3. Топ-10 кращих інструментів OSINT для розвідки з відкритим вихідним кодом. URL: https://ua.softlist.com.ua/articles/top-10-luchshykh-ynstrumentov-osint-dlia-razvedki-s-otkrytym-ishodnym-kodom/ (дата звернення 20.03.2023).

Матвієнко О. В.
доктор педагогічних наук,
кандидат технічних наук, професор,
Київський національний університет культури і мистецтв
Цивін М. Н.
кандидат технічних наук, доцент,
Міжрегіональна академія управління персоналом

ПОТЕНЦІАЛ ВИКОРИСТАННЯ OSINT У ПРОВЕДЕННІ ЗАХОДІВ, ПОВ'ЯЗАНИХ З ІННОВАЦІЙНОЮ РОЗВІДКОЮ

Поміж загроз національній безпеці держави Закон України «Про Національну безпеку» вказує на зниження інноваційної активності і науково-технічного та технологічного потенціалу, скорочення досліджень у стратегічно важливих напрямах інноваційного розвитку. Воєнна агресія проти України актуалізува-

ла питання науково-технічного розвитку, висвітлила критично необхідною науково-технічну діяльність у всіх її формах і видах – науково-дослідні, дослідно-конструкторські, проектно-конструкторські, технологічні, пошукові та проектно-пошукові роботи, а також інші практики, пов'язані з доведенням наукових і науково-технічних знань до стадії практичного їх використання.

Невід'ємною складовою такої діяльності є *інноваційна розвідка* як один із напрямів пошуку нових технологій і рішень. У процесі інноваційної розвідки відбувається вивчення патентів, винаходів, технологій, виявлення фахівців, які беруть безпосередню участь у їх створенні (винахідників, експертів, консультантів, інвесторів), виявлення нових технологічних трендів у наукових публікаціях, в усних виступах фахівців на конференціях та семінарах. Технології інноваційної розвідки по відкритих джерелах (OSINT) спрямовуються також на матеріали конференцій, які вважаються засобом виявлення нових напрямів досліджень, провідних колективів і організацій у певних галузях, встановлюються зв'язки між дослідниками та колективами шляхом аналізу цитування, співавторства тощо.

До терміну «інноваційна розвідка» у синонімічному ряду можуть бути застосовані «технологічна розвідка» («розвідка технологій»), «технологічний скаутинг».

В розробленій у роботі [6] концептуальній моделі *технологічної розвідки* її визначено як збирання і доставка технологічної інформації як частина процесу, за допомогою якого організація розвиває усвідомлення технологічних загроз і можливостей.

На сайті Департаменту внутрішньої безпеки Міністерства національної безпеки США [5] *технологічний скаутинг* (Technology Scouting) окреслено як процес виявлення, визначення місцезнаходження та оцінки наявних або тих, що знаходяться у розробці, технологій, продуктів, послуг та нових тенденцій. Такий підхід дає змогу прискорити розробку і підвищує можливості партнерства і ресурси для допомоги у розробці поточних або майбутніх систем та потреб національної безпеки. Використовуючи науково-технічний персонал, експертів із предметних питань, мережі та бази даних, а також інші інструменти для пошуку в наукових колах, лабораторіях, державних джерелах, приватній промисловості та міжнародній діяльності, технологічний скаутинг надає зведені звіти для підтримки планування програм та інформування про купівлю, будівництво та

змогу адаптувати рішення. Технологічний скаутинг – це збирання інформації про готові комерційні і державні продукти, прототипи, науково-дослідну діяльність і можливості партнерства.

Використовувані як синоніми, згадані терміни часом виокремлюються як самостійні поняття, у працях зарубіжних дослідників обґрунтовується і висвітлюється зв'язок технологічного менеджменту (Technology Management), технологічної розвідки (Technology Intelligence) і технологічного скаутінгу (Technology Scouting) [4].

В Україні діяльність у галузі забезпеченні наукового, науково-технічного та інноваційного розвитку шляхом експертної, інформаційної та консалтингової підтримки здійснюється державною науковою установою «Український інститут науково-технічної експертизи та інформації». Інститутом виконуються дослідження патентної активності за певними напрямами, виконується аналіз світових технологічних трендів, зокрема, у військовій сфері, який оприлюднюється у виді монографій [1; 3].

Разом з тим зазначимо, що узагальнення у монографіях вчених сучасних технологічних трендів, за усієї очевидної необхідності, не відповідає вимогам оперативності монографії як джерела інформації, що потребує безперервного інформаційного моніторингу потоку науково-дослідної, дослідно-конструкторської, патентної та інших видів науково-технічної документації.

Успіх застосування OSINT-технологій у здійсненні інноваційної розвідки безпосередньо залежить від компетентностей аналітика, зокрема його знань системи наукової документації, систем технологічної, конструкторської, патентної документації, джерел та каналів їх одержання [2]. Традиційно, такі знання входять до предметного поля освіти за спеціальністю «Інформаційна, бібліотечна та архівна справа», у межах якої педагогічно доречною та релевантною з теоретико-методологічної точки зору могла б бути спеціалізація «OSINT-аналітика, інноваційна розвідка».

Література

1. Аналіз світових технологічних трендів у військовій сфері : монографія / Т. Писаренко, Т. Кваша, Т. Гаврис та ін.; за заг. редакцією Т. В. Писаренко. Київ: УкрІНТЕІ, 2021. 110 с.

2. Дубова С.В. Науково-технічна документація: методичні рекомендації до вивчення дисципліни. Київ: Центр учбової літератури, 2017. 54 с.
3. Писаренко Т.В. Кваша Т. Глобальні технологічні тренди у сфері озброєння та військової техніки. Київ: УкрІНТЕІ, 2020. 88 с.
4. Rohrbeck R. Technology Scouting – Harnessing a Network of Experts for Competitive Advantage. URL: https://www.researchgate.net/publication/202288895_Technology_Scouting_-_Harnessing_a_Network_of_Experts_for_Competitive_Advantage (дата звернення: 16.03.2023).
5. Technology Scouting. URL: https://www.dhs.gov/science-and-technology/technology-scouting#:~:text=Technology%20scouting%20is%20the%20process,%2C%20services%2C%20and%20emerging%20trends (дата звернення: 16.03.2023).
6. Kerr, C.I.V., Mortara, L., Phaal, R. and Probert, D. R. URL: A conceptual model for technology intelligence. Int. Journal of Technology Intelligence and Planning. 2006. Vol. 2, Issue 1, pp. 73-93.

Благодарний А. М.
доктор юридичних наук, професор,
Національна академія СБ України

УДОСКОНАЛЕННЯ ПРАВОВОЇ РЕГЛАМЕНТАЦІЇ ОДЕРЖАННЯ ІНФОРМАЦІЇ ОРГАНАМИ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Відповідно до Закону України «Про інформацію» кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів.

Стосовно права фізичних осіб на одержання інформації слід зазначити, що основним нормативно-правовим актом у цій сфері є Закон України «Про інформацію», але існують і галузеві закони, що регламентують порядок поширення певної інформації, наприклад, Закон України «Про доступ до публічної інформації», Кодекс цивільного захисту України.

Починаючи розгляд порядку одержання інформації юридичними особами, зокрема органами СБ України, слід зазначити, що Закон України «Про інформацію» містить певні положення щодо одержання інформації зазначеними суб’єктами, однак ці

положення мають багато в чому декларативний характер і переважно розраховані на реалізацію прав громадян, а не юридичних осіб [1, с. 240]. У чинному законодавстві не передбачено спільного механізму отримання інформації різними органами державної влади. Так, І. Сопілко зазначає, що законодавчі та підзаконні нормативно-правові акти містять безліч термінів та конструкцій для формулювання можливостей органів державної влади отримувати інформацію: «отримання відомостей», «одержання інформації», «вилучення документів», «зняття копій» тощо. При цьому не уніфікованими залишаються процедури отримання інформації, у багатьох випадках не передбачається обов'язок власника чи володільця інформації надавати її на законну вимогу органу державної влади, фактично малоефективною залишається юридична відповідальність за ненадання інформації [2, с. 73].

На нашу думку, недосконалість вітчизняного законодавства, що регламентує надання інформації правоохоронним органам, можна пояснити декількома причинами.

По-перше, слід зазначити, що інформаційне право України є відносно молодою галуззю права, і термінологічний апарат ще належним чином не сформувався [3, с. 93]. В. Гурковський, аналізуючи питання інформаційної безпеки, зазначає, що у цій сфері «деякі категорії взагалі не мають чіткого визначення змісту, що призводить до їх неоднозначного трактування на практиці. Наприклад, інформація, таємна інформація, таємниця, документ і документована інформація» [4, с. 177]. У науковій літературі дискутуються не лише питання режиму деяких видів інформації, а навіть їх назви, наприклад, лікарська та медична таємниця [1, с. 241].

По-друге, чинний порядок отримання інформації посадовими особами різних правоохоронних органів, на нашу думку, є занадто різним. У деяких випадках вказується сфера інформації; у деяких – посадова особа, яка має право подавати інформаційний запит; іноді – обставини, при яких має надаватись інформація; іноді – мета, з якою надається інформація; іноді – що інформація має надаватися безкоштовно. Так, відповідно до п. 3 ч. 1 ст. 25 Закону України «Про Службу безпеки України» СБ України, її органам і співробітникам для виконання покладених на них обов'язків надається право: одержувати на письмовий запит

керівника відповідного органу СБ України від міністерств, державних комітетів, інших відомств, підприємств, установ, організацій, військових частин, громадян та їх об'єднань дані і відомості, необхідні для забезпечення державної безпеки України, а також користуватись з цією метою службовою документацією і звітністю. Відповідно до ч. 1 ст. 26 Закону України «Про прокуратуру» прокурор, здійснюючи нагляд за додержанням законів при виконанні судових рішень у кримінальних справах, а також при застосуванні інших заходів примусового характеру, пов'язаних з обмеженням особистої свободи громадян, має право: знайомитися з матеріалами, отримувати їх копії; вимагати від посадових чи службових осіб надання пояснень щодо допущених порушень; знайомитися з матеріалами виконавчого провадження щодо виконання судових рішень у кримінальних справах, робити з них виписки, знімати копії. Відповідно до ч. 1 ст. 33 Закону України «Про Національну поліцію» поліцейський може опитати особу, якщо існує достатньо підстав вважати, що вона володіє інформацією, необхідною для виконання поліцейських повноважень.

Ще однією причиною недосконалості правового регулювання питань надання інформації посадовим особами правоохоронних органів є те, що положення багатьох нормативно-правових актів щодо отримання інформації майже не змінювались з часу прийняття законів про відповідні правоохоронні органи, незважаючи навіть на прийняття Конституції України, Закону України «Про інформацію», а також багатьох інших норм, що регламентують питання інформаційного права, діяльності органів державної влади [3, с. 93, 94]. Так, В. Брижко зазначає, що «сучасне інформаційне законодавство має низку недоліків. Вони зумовлені тією обставиною, що різні закони і підзаконні акти, що регулюють відносини, об'єктом яких є інформація, приймалися в різний час без узгодження понятійного апарату. У юридичній практиці застосовують низку термінів, які не досить коректні, не викликають відповідну рефлексію або не мають чіткого гносеологічного наповнення. Результатом є термінологічна неузгодженість, різне трактування однакових за назвою і формою понять, помилки омонімії, коли застосовують слова, які позначають різни предмети, що призводить до їх неоднозначного розуміння і застосування на практиці» [5, с. 44].

Останнім часом до чинного законодавства були внесені зміни, що сприяють отриманню інформації органами СБ України. Так, нова редакція ст. 185-13 КУпАП (Закон України «Про внесення змін до Кодексу України про адміністративні правопорушення, Кримінального та Кримінального процесуального кодексів України щодо запровадження діяльності Бюро економічної безпеки України та пов'язаного з цим удосконалення роботи деяких державних правоохоронних органів» від 17 листопада 2021 року № 1888-IX) передбачає, зокрема, адміністративну відповідальність за ненадання інформації Службі безпеки України на запит її посадових осіб, надання завідомо недостовірної інформації чи не в повному обсязі, порушення встановлених законом строків її надання, повідомлення третіх осіб стосовно того, що про них збирається така інформація. Вже є відповідна юрисдикційна практика за цією статтею КУпАП, зокрема, вже є судові рішення про притягнення до адміністративної відповідальності за невиконання законної вимоги посадової особи Служби безпеки України щодо надання інформації [6]. Разом із тим, слід зазначити, що на сьогодні масовими проблемами для отримання в установленому порядку певної інформації стало некоректне застосування розпорядниками інформації тимчасової відстрочки у задоволенні запиту на інформацію «до закінчення строку дії воєнного стану в Україні», а не у зв'язку з реальним настанням обставин непереборної сили [7].

Підсумовуючи викладене, слід зазначити, що порядок надання інформації правоохоронним органам має бути більш уніфікованим. Варто погодитися з думкою науковців (наприклад, І. Арістової), які у своїх працях пропонують прийняти Закон України «Про право на інформацію», в якому слід більш чітко визначити права й обов'язки суб'єктів інформаційних відносин [8, с. 230]. Прийняття такого Закону сприятиме вдосконаленню процедури отримання інформації. Вважаємо, що нещодавні зміни у адміністративно-деліктному законодавстві, а також відкриття для доступу Єдиного державного реєстру судових рішень позитивно відобразиться на юрисдикційній практиці щодо притягнення винних осіб до відповідальності за ненадання інформації Службі безпеки України.

Література

1. Благодарний А. М. Концептуальні засади правової регламентації адміністративно-юрисдикційної діяльності органів Служби безпеки України : монографія. Київ : Освіта України, 2020. 304 с.

2. Сопілко І. М. Правове регулювання відносин щодо отримання органами державної влади України інформації : дис. ... канд. юрид. наук : 12.00.07. Київ, 2010. 198 с.

3. Благодарний А. М. Адміністративна відповідальність за відмову в наданні інформації посадовим особам правоохоронних органів. Інформаційна безпека людини, суспільства, держави. 2013. № 2(12). С. 92–96.

4. Гурковський В. І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки : дис. ... канд. наук з держ. упр. : 25.00.02. Київ., 2004. 225 с.

5. Брижко В. М. Про узгодженість понять у сфері інформаційного права. Правова інформатика. 2009. № 1. С. 39–45.

6. Постанова судді Личаківського районного суду м. Львова від 3 листопада 2022 року по справі № 463/7534/22 про адміністративне правопорушення, передбачене ч. 1 ст. 185-13 КУпАП [Електронний ресурс] // Офіційний веб-порталі судової влади України. – Режим доступу : http:// www.reyestr.court.gov.ua (дата звернення: 19.03.2023).

7. Доступ до публічної інформації під час війни: про що говорить судова практика? // Центр демократії та верховенства права : сайт. 27.09.2022. URL: https://cedem.org.ua/analytics/dostup-pid-chas-viyny (дата звернення: 19.03.2023).

8. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти: монографія. Харків: Видавництво Університету внутрішніх справ, 2000. 368 с.

Маренич О. В.
Бюро інформаційної розвідки
при Комітеті кіберрозвідки України,
співзасновник громадської організації «КіберПолк»

ОПРАЦЮВАННЯ ПЕРВИННИХ ДАНИХ, ПОШУК ІНФОРМАЦІЇ У WEB-СЕРЕДОВИЩІ

Кіберволонтерські організації, об’єднання, угруповання грають надважливу роль у пришвидшенні перемоги України. Початок повномасштабної війни росії проти нашої держави активізував не тільки сектор національної безпеки і оборони краї-

ни, а одночасно і кіберволонтерів, які напряму допомагають державним органам. Сьогодення для протистояння актуальним загрозам вимагає від профільних державних органів ефективності, оперативності та професійності, виключної координації з кіберволонтерськими організаціями, угрупованнями. Характерною особливістю російсько-української війни є кіберфронт, заснування та подальша мобілізація кіберволонтерського руху як зі сторони ворога, так і з боку нашої держави. Одним з найпопулярніших напрямків став OSINT.

До задач кіберволонтерів та державних органів сектору національної безпеки безпосередньо відноситься опрацювання первинних даних. Цей процес є важливим етапом збору та аналізу інформації. Профільні державні органи співпрацюють з організаціями, кіберугрупованнями для проведення операцій у напрямку OSINT. Задачі та цілі можуть бути абсолютно різними, починаючи від знаходження інформації про ту чи іншу особу, закінчуючи викриттям агентів, ворожого бізнесу, організацій тощо. Перед проведенням будь-який дій у напрямку OSINT-розвідки спершу потрібно опрацювати наявні дані. Цей процес вимагає врахування достовірності та якості, паралельно проводиться політика зменшення ризиків у виникненні помилок, які можуть принести негативні наслідки в операції. Інструментарієм для опрацювання первинних даних може бути web-середовище, бази даних, інформація від державних органів. Більшість українських OSINT-аналітиків, які знаходяться в рядах кіберволонтерів, мають потужний виклик сьогодення, а саме: проводити якісну розвідку без додаткових інструментів, які можуть допомогти у підвищенні оперативності та ефективності виконання поставлених задач. Проблемою є технічна частина, яка поступово вирішується завдяки тісній співпраці державних органів з організаціями. Пряма координація сектору національної безпеки і оборони України з кіберволонтерами підвищує ефективність виконання завдань, кваліфікаційний рівень двох сторін одночасно. Єдність працівників державних служб, органів з організаціями, угрупованнями створює синтез, який нищить ворога на кіберфронті, особливо в напрямку OSINT-розвідки.

Пошук інформації у web-середовищі є найважливішим етапом у проведенні OSINT-операцій. Інтернет має величезну кількість даних, які можуть допомогти у відкритті криміналь-

них проваджень проти російських загарбників, знаходженні ворожих військових батальйонів, викритті агентів та будь-якої антиукраїнської діяльності. Щоб значно підвищити ефективність пошуку інформації у web-середовищі потрібно:

а) забезпечити анонімність та конфіденційність особистої діяльності в мережі Інтернет. Існують різні варіанти, починаючи від використання VPN, proxy, та закінчуючи користуванням різними браузерами, операційними системи;

б) використовувати різні пошукові системи з правильно побудованими запитами. Завдяки якісному запиту та експлуатації Google Dork можна знайти інформацію різного роду, навіть паролі від ворожих ресурсів з логінами та паролями до адмінпанелей;

в) максимально використовувати соціальні мережі, сервіси, бази даних, бібліотеки, архівні дані, онлайн-форуми тощо;

г) користуватися ліцензованим програмним забезпеченням та сервісами для підвищення ефективності та спрощення процесу знаходження інформації.

Профільні державні органи мають вжити відповідні заходи щодо ліквідації загрози знаходження ворогом чутливої інформації у відкритому доступі про державних працівників та військових, прогалин в державних ресурсах, завдяки яким можна викрасти дані.

Військові реалії абсолютно підтвердили важливість OSINT-розвідки та розуміння цього напрямку в цілому. Військовослужбовці України потребують навчання у напрямку комп’ютерної грамотності та кібербезпеки, тому що ворог не сидить на місці, він щоденно працює проти української державності. Сьогодні захисники нашої країни під прицілом російських OSINT-аналітиків, які проводять моніторинг українського web-середовища. Виключно завдяки плідній праці ми зможемо не тільки підвищити кваліфікованість, професійність, ефективність української OSINT-розвідки, а й перемоги реваншистську, імперіалістичну російську державну військову машину.

Бондаренко О. Г.
доктор наук з державного управління, доцент
Луговський І. С.
кандидат військових наук, доцент,
Національна академія Національної гвардії України
(м. Харків)

АКТУАЛЬНІ ПИТАННЯ ВИКОРИСТАННЯ ОТРИМАНОЇ ЗАСОБАМИ OSINT РОЗВІДУВАЛЬНОЇ ІНФОРМАЦІЇ В ОРГАНАХ ВІЙСЬКОВОГО УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ ПІД ЧАС ВІДСІЧІ ЗБРОЙНОЇ АГРЕСІЇ

Досвід бойових дій в сучасних військових конфліктах неодноразово підтверджував важливість організації усіх можливих видів розвідки та використання способів її ведення. Одним із таких видів розвідки є розвідка на основі відкритих джерел (англ. *Open source intelligence, OSINT*) – концепція, методологія і технологія добування і використання військової, політичної, економічної та іншої інформації з відкритих джерел, без порушення законів, яка включає в собі: пошук інформації, її реєстрацію, облік та аналіз, аналітико-синтетичну переробку первинної інформації, зберігання й розповсюдження інформації, забезпечення безпеки інформації та презентацію результатів досліджень.

Крім того, протягом воєнних конфліктів XXI століття спостерігалися закономірні одночасні зміни у способах ведення збройної боротьби та організації розвідки в її інтересах. Зміщення способів протистояння у бік комплексної боротьби у свою чергу спрямовують у цьому напрямку і розвиток способів ведення розвідки. Набутий досвід в організації та ведені розвідки під час російсько-української війни вказує на можливість використання результатів розвідки тактичного рівня позитивно вплинути на хід операції угруповання військ сил оборони України.

З початком широкомасштабного вторгнення збройних сил російської федерації на територію України великої актуальності набуло добування розвідувальних відомостей від місцевого населення та з відкритих джерел інформації. Добування розвідувальних відомостей від місцевого населення та з відкритих джерел інформації відноситься до заходів особової розвідки.

Під особовою розвідкою розуміється комплекс заходів і дій, що здійснюється визначеними підрозділами з використанням способів добування відомостей від людських ресурсів (джерел) з метою забезпечення органів військового управління (штабів) розвідувальною інформацією в інтересах підготовки і ведення бойових (спеціальних) дій військовими частинами (підрозділами) сил оборони України. Особова розвідка ведеться шляхом використання особових та неособових джерел інформації (відкриті джерела інформації, документи та зразки ОВТ противника).

Основними завданнями особової розвідки є: добування розвідувальної інформації про сили і засоби противника та його наміри з метою забезпечення ведення бойових (спеціальних) дій військовими частинами та підрозділами; добування розвідувальної інформації про об'єкт, зону (район) бойових (спеціальних) дій з метою забезпечення заходів безпеки застосування військових частин та підрозділів, в інтересах яких вони діють; збір розвідувальної інформації з метою оцінювання результатів бойових (спеціальних) дій; розвідка місцевості та інфраструктури у районах дій військ; отримання розвідувальної інформації з відкритих джерел; проведення аналізу добутої первинної розвідувальної інформації, тенденцій змін обстановки в зоні (районі) ведення бойових (спеціальних) дій; пошук та виявлення перспективних осіб.

Досвід організації та здійснення заходів особової розвідки в інтересах розвідувального забезпечення операцій угруповання військ сил оборони нашої держави з відсічі збройної агресії російської федерації, дозволяє зробити висновки, що розвідка з відкритих джерел, зокрема, дії населення з документування та розповсюдження інформації про дії противника суттєво сприяють підвищенню спроможностей розвідувального забезпечення дій наших військ в цих операціях.

Водночас, основними умовами ефективного використання отриманої розвідувальної інформації в органах військового управління Національної гвардії України є:

створення систем аналізу інформації та єдиного центру її обробки; скорочення часу проходження інформації від першоджерела до центру обробки;

забезпечення належної якості первинної обробки інформації (фото, відео фіксація тощо);

спроможність органів військового управління приймати, обробляти та використовувати зазначену інформацію.

Подальший розвиток спроможностей особової розвідки в Національній гвардії України можливий такими шляхами:

створення програмного забезпечення із захищеними каналами передачі даних, які доступні для використання на поширених абонентських телекомунікаційних пристроях (терміналах) на базі Android, IOs, Windows, з вбудованою функцією швидкого видалення цього програмного забезпечення та слідів передачі даних;

розгортання резервних мереж передачі даних, наприклад, Starlink на випадок знищення (подавлення) основних телекомунікаційних мереж;

впровадження систем інтелектуального розпізнавання даних в роботу центрів збору та обробки інформації: фото-, відео-, зокрема, розпізнавання обличь, техніки, місцевих орієнтирів, форм документів тощо.

Штаненко С. С.
кандидат технічних наук, доцент,
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут

ПРОГРАМОВАНА ЛОГІКА ЯК СПОСІБ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ СУЧАСНИХ УПРАВЛЯЮЧИХ СИСТЕМ ВІД АПАРАТНИХ ЗАКЛАДОК

Сучасні управляючі системи різного призначення (автоматизовані системи управління – АСУ, автоматизовані системи управління технологічними процесами – АСУ ТП тощо) відносяться до об’єктів критичної інформаційної інфраструктури. При цьому данні об’єкти в якості основних елементів містять засоби обчислювальної техніки – процесори, блоки пам’яті, перетворювачі, датчики, вимірювальні та виконавчі пристрої, елементною базою яких є інтегральні схеми.

Відповідно до класифікації [1] інтегральні схеми (ІС) поділяються на цифрові, аналогові та аналогово-цифрові. У свою чергу, цифрові ІС поділяються на стандартні та спеціалізовані. Стандартні ІС мають практично жорстку внутрішню структуру,

без впливу на характер їх функціонування. Спеціалізовані ІС мають індивідуальний характер функціонування, при цьому доводиться тією чи іншою мірою їх розробляти під конкретне замовлення. У цьому напрямі найважливішим досягненням стало поява програмованих логічних інтегральних схем (ПЛІС).

Слід зазначити, що у зв'язку з глобалізацією і складністю ІС, а також з урахуванням масового використання в різних галузях людської діяльності на перший план виходить проблема надійного та безпечного їх функціонування. А це в свою чергу пов'язано із забезпеченням не лише кіберстійкості цифрових пристроїв та обчислювальних систем, а також із забезпеченням захищеності життєво важливих інтересів людини і громадянина, суспільства та держави. Саме без вирішення цієї проблеми цифрові пристрої та обчислювальні системи не зможуть повноцінно виконувати покладені на них функції, крім цього можуть виступити провідником кібератак на управляючі системи.

Зазначимо, що в останні роки з'явилися нові потенційні загрози безпеці в даній сфері, які базуються на апаратних засобах, – так звані апаратні закладки або апаратні трояни, які є навмисною зловмисною модифікацією електричної схеми або її конструкцією, що призводить до неправильного функціонування цифрових пристроїв та обчислювальної системи. Подібно до програмної закладки (програмного трояну), апаратна закладка представляє собою свого роду чорний вхід в цифровий пристрій. При цьому апаратний троян має додаткову перевагу – він постійно присутній на найнижчому рівні обробки інформації, що веде до збереження загроз відмови або відхилення від нормального функціонування ІС протягом усього часу використання цифрового пристрою або обчислювальної системи. Апаратна закладка може тривалий час залишатися бездіяльною та активуватися самостійно або за допомогою програмного забезпечення, у яке навмисно закладена така можливість.

Апаратні закладки є відносно новими загрозами для кібербезпеки, при цьому вони суттєво розширюють можливості для атаки на технологічні системи. Раніше атаки обмежувалися лише програмними засобами, зосереджуючись на слабких місцях програмного забезпечення. При цьому засоби захисту конкретного програмного забезпечення розроблялися виходячи з автентичності апаратного забезпечення, тому загальноприйняті підходи до захисту програмними засобами не здатні забезпечити

безпеку від апаратних троянів. З цього погляду апаратні закладки є досить складною проблемою забезпечення безпеки сучасних управляючих систем.

Виходячи з сказаного одним із підходів до надійного та безпечного функціонування сучасних управляючих систем, здатних протистояти шкідливим атакам, є застосування в якості елементної бази інтегральних схем з програмованою структурою, тобто ПЛІС.

Програмовані логічні інтегральні схеми є матрицею програмованих логічних елементів з *SPLD* (*Simple Programmable Logic Devices*), *CPLD* (*Complex Programmable Logic Device*), *FPGA* (*Field-Programmable Gate Array*), *FLEX* (*Flexible Logic Element Matrix*) структурами. За рахунок цих структур створюється новий клас розвитку мікроелектроніки – універсальні системи на кристалі (*System-on-Chip – SoC*).

Система на кристалі або *SoC* представляє собою обчислювальну систему, реалізовану в інтегральному виконанні, до складу якої входить високопродуктивний процесор або декілька процесорів, математичний процесор обробки даних та цифрової обробки сигналів, додаткові модулі пам'яті, набори периферійних пристроїв (контролерів) тощо. Така організація обчислювальної системи набула широкого поширення за допомогою своєї універсальності, малого енергоспоживання і навіть можливості реконфігурації її алгоритмічної структури. Зазначимо, що на сьогодні системи на кристалі витісняють громіздкі обчислювальні структури, реалізовані за допомогою набору інтегральних схем, замінюючи їх сучасними мікроконтролерами (*PIC*, *AVR*, *MSP*430, *STM*-32, *Cortex-M*, *TSP*-32 тощо), програмованими логічними інтегральними схемами (ПЛІС – *CPLD*, *FPGA*, *FLEX*) та одноплатними комп'ютерами типу *Raspberry Pi* [2].

Слід зазначити, що на відміну від стандартних ІС, логіка роботи ПЛІС не визначається при виготовленні, а задається шляхом програмуванням. Для цього використовуються програматор та інтегроване середовище розробки (*IDE – Integrated Development Environment*), що дозволяють задати бажану структуру цифрового пристрою у вигляді принципової електричної схеми або програми спеціальними мовами опису апаратури *Verilog*, *VHDL*, *AHDL*.

Так, згідно [3] саме застосування ПЛІС у якості елементної бази побудови сучасних управляючих систем відкриває нові

можливості щодо підвищенні кіберстійкості цифрових пристроїв та обчислювальних систем до кібератак, як програмного, так і апаратного характеру. В основі даного підходу лежить принцип реалізації активної відмовостійкості, який включає наступні етапи: виявлення відмови (кібератаки) шляхом застосування існуючих методів контролю технічних засобів; локалізація відмови (реагування на кібератаки) шляхом застосування методів тестового та функціонального діагностування; відновлення правильного функціонування системи шляхом реконфігурації її внутрішньої структури на рівні логічних елементів. При цьому зазначимо, що в основу реконфігурації внутрішньої структури цифрових пристроїв та обчислювальних систем покладене положення прескриптивної теорії, яка розглядає питання цілеспрямованого управління об'єктами різної природи, що перебувають у стані «конфлікту» з іншими об'єктами [4].

Таким чином, реалізувавши принцип активної відмовостійкості на сучасній програмованій елементній базі, ми маємо можливість протидіяти не лише кібератакам програмного і апаратного характеру на цифрові пристрої та обчислювальні системи, а й підвищити кіберстійкість управляючих систем загалом.

Література

1. Engr Fahad. Types of Integrated Circuits, Classification of ICs by Structure. URL: https://www.electroniclinic.com/types-of-integrated-circuits-classification-of-ics-by-structure/ (дата звернення 15.03.2023).

2. Saleh, Reyad & Wilton, Steve & Mirabbasi, Shahriar & Hu, Alan & Greenstreet, Mark & Lemieux, Guy & Pande, Partha & Grecu, Cristian & Ivanov, Andre. (2006). System-on-Chip: Reuse and Integration. Proceedings of the IEEE. 94. 1050–1069. 10.1109/JPROC.2006.873611.

3. Штаненко С. С. Адаптація мікропроцесорних систем управління до несприятливих впливів / С. С. Штаненко, Ю. Я. Самохвалов // Сучасна спеціальна техніка: ДНДІ МВС України. Київ. 2022. № 3(70). С. 89–100. ISSN: 2411-3816.

4. Обухов В. Е. Синтез избыточных дискретных устройств с реконфигурацией структуры / В. Е. Обухов, В. В. Павлов. Киев: Наукова думка, 1979. 156 с.

Варжанський І. В.
Національний технічний університет України
«КПІ імені Ігоря Сікорського»

ВИЯВЛЕННЯ ЗА ДОПОМОГОЮ ЗАСОБІВ OSINT ОСІБ, СХИЛЬНИХ ДО СПІВПРАЦІ З ВОРОГОМ

Розвідка з відкритих джерел інформації (OSINT) в останні десятиліття стає все більш популярним інструментом в різних галузях, в першу чергу в секторі безпеки та оборони. Для перевірки певної особи, органи державної безпеки традиційно спираються на закриті джерела, такі як агентурні та оперативно-технічні заходи, візуальне спостереження тощо. Ці методи можуть надати цінну інформацію про індивідуальні контакти, спосіб життя, фінансову стабільність і поведінку людини, які можуть вказувати на схильність до підготовки і вчинення злочинів проти національної безпеки. Однак з появою соціальних мереж та інших онлайн-платформ, де процеси аналізу можуть бути автоматизовані, а відтак масштабовані, OSINT стає незамінним інструментом для виявлення потенційних загроз на ранніх стадіях.

Досвід російсько-української війни з 2014 показує, що цілями диверсій можуть бути не лише військові об’єкти, але і цивільна критична інфраструктура на всій території країни. Метою таких терористичних атак є підрив економіки та психоемоційного стану населення країни. За стратегічними об’єктами, вогневе ураження яких ракетними ударами або тільки готується, або неможливе чи недоцільне до певного моменту, необхідне регулярне спостереження. В глибокому тилу воно може здійснюватися засобами космічної розвідки, за допомогою перехоплення інформації з телекомунікаційних мереж або з відкритих джерел. Але є підстави вважати, що найпоширенішим шляхом отримання таких розвідувальних даних залишається застосування агентурних мереж, зокрема громадян, які проживають в районах розміщення потрібних об’єктів. Вербування цивільних осіб для виконання диверсійно-розвідувальних завдань на такому рівні потребує масовості, відповідно мотиви вербування, як правило, обмежуються ідеологічними та матеріальними. При цьому комунікація як на етапі вербування, так і при супроводі роботи агента може відбуватися дистанційно через телекомуні-

каційні засоби. Отже, для профілактичної роботи з виявлення осіб, які можуть бути вразливі до вербування та схильні до створення загроз національної державності, можливо за допомогою технологій OSINT збирати дані про користувачів соціальних мереж за низкою критеріїв, які є індикаторами ризиків (за принципом «скорингу»).

Ми визначили так основні групи індикаторів, які можуть свідчити про схильність особи до диверсійно-розвідувальної роботи і при цьому можуть бути виявлені автоматично:

- ідеологічні;
- кримінальні;
- фінансові;
- психопатологічні.

Розглянемо кожну групу індикаторів окремо. Ідеологічні індикатори свідчать про прихильність користувача соціальної мережі до якоїсь ідеї, наприклад концепції «русского мира» або релігійного екстремізму. Прихильність може виражатися у масовій підписці на спільноти певної спрямованості, вподобаннях, репостах та коментарях. Слід розуміти, що в умовах ідеологічно ворожого середовища людина може бути раціонально схильна приховувати свою позицію, а перелічені маркери є досить очевидними для більшості досвідчених користувачів соціальних мереж. Тому, якщо в загальному випадку більше сигналів (вподобань, репостів, підписок) буде свідчити про більшу ймовірність прихильності користувача до відповідної ідеї, не слід також виключати ймовірність прихованої прихильності у випадку навіть кількох або одного характерного сигналу (наприклад, єдиний коментар, який користувач забув видалити). Ця метрика може здаватися суперечливою з етичної точки зору, якщо дії користувача в соціальній мережі безпосередньо не порушують законодавство, але окремо навіть значна кількість сигналів не може бути приводом для процесуальних дій – вони є лише елементом комплексної системи аналізу ризиків. Технічна реалізація залежить від соціальної мережі, де проводиться моніторинг. «Twitter» надає у відкритому вигляді дані про нові коментарі та вподобання користувача, «Facebook» дає можливість знаходити коментарі через вбудовану функцію пошуку, «Instagram» дозволяє без застосування спеціальних сервісів виявити лише підписки. Деякий інтерес становлять заборонені в Україні соціальні мережі «Вконтакте» та «Одноклассники», де в покинутих про-

філях можуть бути відображені політичні переконання особи, які вона с певного моменту після 2017 року почала приховувати. Сканування за списками «друзів» та підписок на кілька рівнів глибини дозволяє виявити вподобання та коментарі у тих соціальних мережах, де у відкритому вигляді така функція не передбачена.

Схильність до кримінальної діяльності може бути виявлено за аналогічними показниками – відповідні тематичні публікації на власних сторінках та підписка на спільноти кримінальної спрямованості. Особливий інтерес у цьому контексті представляє месенджер «Telegram». Завдяки підвищеній анонімності та широкому функціоналу, можна констатувати, що «Telegram» став однією з найпопулярніших платформ для злочинної діяльності в інтернеті [1], особливо серед початківців. Технічно взаємодія між кримінальними елементами на платформі здійснюється особисто, а також через канали та чати. Формат каналів необхідний для рекламування послуг, чати виконують аналогічну функцію, проте більшість стійких спільнот має додаткову перевагу для учасників – вони мають регулювання. Контроль за виконанням зобов'язань у формі «гаранта» та арбітражу є найбільш раціональним у тіньовій сфері, як було показано у низці наукових досліджень [2, с. 6]. Все це призводить до того, що зацікавлені в незаконному збагаченні особи, які мають хоча б базові навички у сфері інформаційних технологій, рано чи пізно з високою ймовірністю виявляють та долучаються до тіньових чатів у «Telegram» або інших злочинних спільнот у deep та dark web. Парсинг учасників цих чатів, щонайменше у рамках месенджера «Telegram», не потребує спеціальних технологій та суттєвих ресурсів. Слід зазначити, що такі послуги, як, наприклад, підпал автомобіля приватної особи, є звичайною пропозицією у згаданих спільнотах, а виконавці «замовлень» можуть не володіти ресурсами або мотивацією для перевірки об'єкта атаки, таким чином використовуватися несвідомо.

Одним із поширених чинників, які штовхають громадян до державної зради, є важке фінансове становище. В умовах тривалої економічної кризи, неминучої в період війни та повоєнної відбудови, значна частка населення може зіткнутися з втратою джерел доходу та нестачею коштів для забезпечення свого існування. Це полегшує завдання вербування, щонайменше для збору інформації. Хоча користувачі соціальних мереж зазвичай не

публікують інформацію про свої фінансові проблеми, але інформацію про таких громадян легко отримати через відкриті дані виконавчої служби, судові реєстри та інші бази даних, які використовуються для перевірки ділової репутації. Інформація там має високу достовірність, включає персональні дані, конкретні суми заборгованості та часто навіть дозволяє приблизно встановити місце проживання об'єкта. Хоча лише наявність фінансових проблем може бути недостатньо надійною підставою для вербування, такий індикатор є вкрай важливим для врахування в загальній системі оцінки ризиків, особливо якщо він поєднується з індикатором з іншої групи.

Група індикаторів психопатології у користувачів соціальних мереж є найскладнішою в автоматичному виявленні. Зазначимо лише основні перспективні напрямки для такого аналізу: пошук серед публікацій користувача за ключовими словами та фразами, що відповідають поширеним теоріям глобальної змови, неконструктивним скаргам чи погрозам, масова підписка на відповідні спільноти та активні репости їх змісту, загальна неприродня частота публікацій чи коментарів, особливо агресивної тональності. На сучасному етапі розвитку технологій машинного навчання, такі моделі, як GPT-4, вже можуть використовуватися для виявлення психологічних аномалій в повідомленнях користувача із задовільною точністю. Важливо, що жоден із цих індикаторів не гарантує наявність психічного розладу у користувача соціальної мережі, і лише діагностика фахівця може дати точний висновок. Особи, у яких виражені психічні захворювання, можуть бути виявлені агресором та віддалено завербовані за допомогою методів соціальної інженерії для збору інформації або здійснення теракtів [3].

Окремою категорією індикаторів, яка входить до групи психопатологічних, є наркозалежність. Методи виявлення наркозалежності перетинаються з методами, які ми описали для групи кримінальних індикаторів. Істотна частина користувачів відповідних тематичних чатів чи каналів нелегальних торгових майданчиків у месенджерах є регулярними покупцями наркотиків, складність становить лише завдання відокремлення споживачів легких від важких наркотиків, оскільки саме вживання останніх пришвидшує психологічний розпад особистості та, відповідно, збільшує ймовірність вербування. Іноді користувачі самі розповідають про своє «дозвілля» в профілях соціальних

мереж, згадують характерні ключові слова або використовують відповідні ідеограми «емодзі». Автоматична оцінка ймовірності наявності психічного розладу чи наркозалежності у користувача соціальної мережі є перспективним напрямом OSINT, дослідження у цьому напрямі можуть бути продовжені у наступних роботах.

Певною мірою всі учасники кримінальних Інтернет-спільнот та схильні до співпраці з ворогом на підставі ідеологічних міркувань особи, а тим паче екстремісти, становлять інтерес для правоохоронних органів, проте в рамках здійснення контррозвідувального захисту національної державності, раціональним вбачається подальша фільтрація списків цих користувачів. Нами пропонується звуження вибірки осіб шляхом перевірки геолокації та належності до категорій осіб, які є пріоритетними для забезпечення контррозвідувального захисту національної державності, наприклад військовослужбовців, працівників критичної інфраструктури, громадян, що мають доступ до державної таємниці тощо.

Для частини користувачів «Telegram» геолокацію можливо встановити декількома найменш трудомісткими методами: якщо у них увімкнена вбудована функція Telegram «Знайти людей поряд» (транслюють своє місце розташування), або номери їх телефонів не приховані, або номери телефонів їх облікових записів потрапили у базах даних витоків. Також в інших соціальних мережах геолокація може бути встановлена за геомітками фотографій, за ключовими словами, а місце роботи також може бути встановлено статистичним методом – ймовірно, воно буде співпадати з місцем роботи більшості «друзів».

Ті користувачі, які мають вороже ставлення до національної державності України або екстремістські погляди, схильні до протизаконної діяльності або виявляють ознаки значних психічних розладів, їхнє розташування встановлено і воно відповідає районам розташування об'єктів критичної інфраструктури, або вони мають доступ до стратегічно важливої інформації, представляють групу ризику. Видається виправданим проведення роботи засобами OSINT, оперативних комбінацій на каналах телекомунікаційних мереж та оперативно-технічних заходів для їх подальшої ідентифікації та профілактики. Зворотній, більш традиційний, підхід полягає в автоматизації аналізу за встановленими індикаторами ризику соціальних мереж для певних ка-

тегорій осіб, зокрема тих, що мають доступ до державної таємниці. Аналіз може здійснюватися як при наданні допуску до державної таємниці або при працевлаштуванні, так і приймати форму постійного моніторингу акаунтів у соціальних мережах та месенджерах для своєчасного виявлення зміни поведінки, що може призвести до збільшення ступеня ризику.

Водночас проблема пошуку ворожих агентурних мереж може мати ознаки культурного феномену у спільнотах, де зберігається пам'ять про тоталітарні періоди історії держави та відповідні психологічні наслідки, пов'язані з історичною травмою, ще не були повністю подолані. Іноді такі спільноти більш схильні до масової параної у формі так званої шпигуноманії. Цим може користуватися агресор, нагнітаючи серед органів влади та цивільного населення істерію шляхом проведення інформаційно-психологічних операцій про нібито наявність великої кількості завербованих інформаторів або диверсантів. Прикладом такої операції вбачається створення у лютому 2022 року низки ресурсів, зокрема в месенджері Telegram, в яких відрито розповсюджувалися заклики до нанесення «міток», розміщення ліхтарів та GPS-маяків в українських містах [4][5].

Висновки. OSINT є потужним інструментом для профілактичних заходів із забезпечення контррозвідувального захисту національної державності. Моніторинг соціальних мереж для виявлення в регіоні осіб, схильних до вербування, може бути одним із важливих елементів комплексної системи оцінки ризиків для підприємств критичної інфраструктури. Представлені групи індикаторів не охоплюють усі можливі причини для колабораціонізму, оскільки деякі з них не відображаються у відкритих джерелах і не можуть бути виявлені автоматично. У подальших дослідженнях може бути доповнено кількість груп індикаторів та методів їх виявлення. Крім того, слід пам'ятати, що наведені індикатори є лише елементами системи оцінювання ризиків, а робота і, певною мірою, мистецтво працівників підрозділів захисту національної державності полягає у точному виявленні справжніх агентів, незважаючи на активні дезінформаційні заходи агресора.

Література

1. KELA CYBERCRIME INTELLIGENCE. Telegram: How a messenger turned into a cybercrime ecosystem by 2023. 2023. 60 с. URL:

https://ke-la.com/wp-content/uploads/2023/02/KELA_Telegram_CEBIN.pdf (дата звернення: 19.03.2023).

2. Jung B. R., Choi K.-S., Lee C. S. Dynamics of Dark Web Financial Marketplaces: An Exploratory Study of Underground Fraud and Scam Business. *CrimRxiv*. 2022. URL: https://doi.org/10.21428/cb6ab371.dbbe560f (дата звернення: 19.03.2023).

3. Ritzmann A. Islamismus: Wie Terroristen Behinderte missbrauchen - WELT. *DIE WELT*. URL: https://www.welt.de/politik/article2064205/Wie-Terroristen-Behinderte-missbrauchen.html (дата звернення: 19.03.2023).

4. Ukrinform. Сучасна військова техніка не здійснює наведення по мітках на стовпах і дорогах - Арестович. *Укрінформ*. URL: https://www.ukrinform.ua/rubric-ato/3414633-sucasna-vijskova-tehnika-ne-zdijsnue-navedenna-po-mitkah-na-stovpah-i-dorogah-arestovic.html (дата звернення: 19.03.2023).

5. Пономаренко М. Федоров розповів, чому мітки для наведення ракет стали неефективними для росіян. *24 Канал*. URL: https://24tv.ua/fedorov-rozpoviv-chomu-mitki-dlya-navedennya-raket-stali-neefektivnimi_n1964145 (дата звернення: 19.03.2023).

Артамонов Є. Б.
кандидат технічних наук, доцент
Крант Д. В.
Національний авіаційний університет
Данкович Н. І.
Національна академія СБ України

МОЖЛИВОСТІ ІДЕНТИФІКАЦІЇ ВОДІЯ ЗА СТИЛЕМ ЙОГО ВОДІННЯ

Автоматизовані системи технічних засобів з кожним роком стають все більш розповсюдженими і комплексними. Зокрема, вони дозволяють віддалено контролювати і керувати технічними засобами [1], встановлюються системи допомоги при паркуванні, системи відеоспостереження, навігаційні системи, навіть керування системами ведення вогню на військовій техніці. При цьому, всі ці системи потребують передачі даних між собою і зовнішнім світом.

Розробка автоматизованих систем управління автомобілями та їх підключення до мережі дозволяють створити нові можливості для взаємодії між технічними засобами, дорожніми інфра-

структурами та іншими сервісами. Проте, це також викликає проблеми щодо забезпечення безпеки передачі даних, оскільки зловмисники можуть зламати системи та отримати несанкціонований доступ до даних, що може призвести до серйозних наслідків [2].

Однією з небезпек є можливість віддаленого керування автомобілем. Це може бути зроблено через несанкціонований доступ до системи технічного засобу, що може призвести до того, що зловмисник зможе керувати технічним засобом з метою завдання шкоди. Крім того, можлива зміна даних в системах технічного засобу, що може призвести до збоїв в роботі та втрати контролю.

Окремою задачею стоїть ідентифікація водія за даними бортового комп'ютера. Ці дані можуть використовуватись як при розслідувані окремих випадків на дорогах, так і для ідентифікації водіїв при воєнних розслідуваннях, коли свідки відсутні.

Ще одна проблема безпеки полягає у збереженні та передачі особистих даних, таких як геолокація, інформація про водія та пасажирів, інформація про маршрути та інші дані. Ці дані можуть бути використані для здійснення кібератак або ж для здійснення крадіжок та інших злочинів.

Окрім того, зростає кількість смарт-пристроїв, які можуть бути підключені до систем технічних засобів, таких як смартфони, планшети та інші. Це створює додаткові точки входу для зловмисників, які можуть використовувати ці пристрої для здійснення атак на системи управління.

Методи ідентифікації водія за його поведінкою, такі як манери їзди, використання підключених пристроїв та програм, стають все більш популярними в автомобільній промисловості [3–5]. Такі методи можуть забезпечувати вищий рівень безпеки та стійкості до атак зловмисників, дозволяти проводити розслідування і збирати достовірну аналітику, оскільки вони дозволяють ідентифікувати водія за його унікальними характеристиками.

Один з можливих методів аутентифікації – аналіз манер їзди водія. Цей метод полягає в тому, щоб збирати та аналізувати дані про стиль водіння, такі як швидкість, прискорення, гальмування, повороти та інші параметри [6]. Ці дані можуть бути зібрані за допомогою датчиків, які встановлені в технічному засобі, а потім оброблені за допомогою аналітичного програмного

забезпечення для ідентифікації конкретного водія. Для цього можна використовувати машинне навчання та штучну інтелект для розпізнавання унікальних особливостей кожного водія.

В моделі поведінки водія можуть використовуватися різноманітні параметри, такі як швидкість руху, частота гальмування, кут повороту керма, час реакції на сигнали дорожнього руху, та інші. Ці параметри можуть бути оброблені та порівняні зі значеннями, які раніше були збережені в системі для підтвердження ідентифікації водія.

Модель поведінки водія може бути представлена у вигляді матриці *X*, де кожен рядок містить значення параметрів поведінки водія, або у вигляді вектору x, який містить значення параметрів поведінки водія для одного конкретного моменту часу.

Також можуть використовуватися різні методи машинного навчання [7], такі як класифікація, кластеризація, нейронні мережі, щоб навчити систему розрізняти поведінку різних водіїв та визначати, чи є водій авторизованим для керування конкретним автомобілем.

Проаналізуємо вхідні дані, які можна використовувати для аутентифікації водія через аналіз його поведінки:

– для розрахунку параметрів манери водіння, можна використати датчики в технічному засобі для вимірювання швидкості, прискорення та гальмування;

– для параметрів використання підключених пристроїв та програм, можна використовувати датчики, що виявляють підключення до портів технічного засобу або програм, встановлених на мобільних пристроях;

– для параметрів фізіологічні характеристики водія, можна використовувати датчики, що вимірюють ритм серця та інші фізіологічні показники;

– для параметрів контексту водіння, можна використовувати датчики, що вимірюють тип дороги, швидкість руху та інші показники.

Дослідження показало, що існують різні методи ідентифікації водія за стилем його водіння, що дозволяє використовувати ці дані, як в системах безпеки технічного засобу і вживати заздалегідь прописані сценарії, так і для аналізу даних бортових комп’ютерів сторонніми експертами під час розслідувань чи уточнення аналітичних даних.

Література

1. Ali Alheeti KM, Gruebler A, McDonald-Maier K. 2016. Intelligent intrusion detection of grey hole and rushing attacks in self-driving vehicular networks. Computers 5(16).

2. Alnasser A, Sun H, Jiang J. 2019. Cyber security challenges and solutions for V2X communications: A survey. Computer Networks 151:52–67.

3. Artamonov Y., Golovach I., Krant D., Rosinska H., Nechyporuk O., Stanko S. Dynamic Content Generation Methods Based on User Behavioral Ranking, 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 313-318, doi: 10.1109/ATIT58178.2022.10024196.

4. Stylios I., Kokolakis S., Thanou J. Chatzis S. Behavioral biometrics & continuous user authentication on mobile devices: A survey // Information Fusion. –Volume 66. – 2020. – pp. 76-99. https://doi.org/10.1016/j.inffus.2020.08.021.

5. Wong-In S., Netinant P. Designing an examinee personal verification system using biometric technology // J. Curr. Sci. Tecnnol. – 2018. – № 8. – pp. 75–86.

6. Aloqaily M, Otoum S, Al Ridhawi I, Jararweh Y. 2019. An intrusion detection system for connected vehicles in smart cities. Ad Hoc Networks 90:101842.

7. Ahmed, A.A. Future effects and impacts of biometrics integrations on everyday living // Al-Mustansiriyah J. Sci. – 2019. № 29. – pp. 139–144.

Дашковська А. В.
Національна академія внутрішніх справ

ІНФОРМАЦІЙНО-АНАЛІТИЧНА СИСТЕМА «СОТА» ЯК ІНСТРУМЕНТ АНАЛІЗУ ТА УПРАВЛІННЯ РИЗИКАМИ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ

Рада національної безпеки і оборони України з метою підвищення ефективності інформаційно-аналітичного забезпечення прийняття управлінських рішень, взаємодії, координації і контролю за діяльністю органів виконавчої влади, правоохоронних органів та військових формувань у сферах національної безпеки і оборони у мирний час, а також в особливий період, у тому числі в умовах воєнного стану, в умовах надзвичайного стану та під час виникнення кризових ситуацій, що загрожують національній безпеці України розширює та розвиває єдину ме-

режу ситуаційних центрів. Президент України своїм Указом від 18 червня 2021 року № 260 ввів у дію Рішення Ради національної безпеки і оборони України від 4 червня 2021 року «Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони».

Зазначені центри оснащуються уніфікованим програмним та апаратним забезпеченням із інформаційно-аналітичного супроводження прийняття управлінських рішень, яке включає:

- сховище даних та систему керування базами даних;
- інструменти аналізу та візуалізації даних від різних джерел, а також побудови прогностичних моделей на їх основі;
- модуль геоінформаційних систем і технологій для створення та роботи з наборами геопросторових даних;
- захищений відеоконференцзв'язок для забезпечення синхронного обміну аудіовізуальною інформацією в режимі реального часу;
- електронні комунікаційні мережі для забезпечення обміну інформацією, включаючи передачу даних та аудіовізуальної інформації з різними ступенями обмеження доступу між комунікаційними вузлами, ситуаційними центрами та іншими суб'єктами інформаційного обміну;
- технічну підтримку програмно-апаратного комплексу для забезпечення інтероперабельності, стійкого і безперервного функціонування, тестування, конфігурації та відстеження продуктивності згідно з визначеним регламентом [1].

Об'єднані в єдину захищену мережу, ситуаційні центри оперативно оброблятимуть інформацію, аналізуючи її прийматимуть критично важливі для держави рішення. Наразі, в Апараті РНБО України діє Головний ситуаційний центр України, а також ситуаційні центри низки ключових державних органів сектору безпеки і оборони.

Сучасна інформаційно-аналітична система Головного ситуаційного центру країни «СОТА» працює з Big Data, забезпечує зберігання, поєднання та аналіз даних з різних джерел задля підвищення достовірності, ефективного моніторингу стану національної безпеки по понад 20 напрямах, з метою ефективної координації діяльності державних органів. ІАС «СОТА» – дієвий інструмент, яким користується вище керівництво держави при прийнятті управлінських рішень.

Серед цих напрямів – соціальна, внутрішньо- та зовнішньополітична безпека, російсько-українська війна, поширення захворюваності на коронавірусну інфекцію COVID-19 у світі та в Україні, просторова та функціональна трансформація, самоврядування у контексті децентралізації, місцеві бюджети та спроможність громад, надрокористування, економічна безпека, фінансові ринки, загрози на внутрішніх та зовнішніх ринках тощо [2].

Основними напрямами здійснення моніторингу Апаратом РНБО стану національної безпеки на сьогодні є:

- воєнна безпека;
- громадська безпека;
- економічна;
- соціальна;
- екологічна складова.

Фахівцями Апарату РНБО розроблений також портал щодо воєнних злочинів рф, який включає, з-поміж іншого, дані космічної зйомки. При цьому вся інформація, яка збирається із зовнішніх джерел і обробляється у системі, синхронізована з геопросторовими даними.

Технологія пошуку та аналізу інформації з відкритих джерел здавна використовується в роботі розвідок багатьох країн. Особливо активно в Україні заговорили про це після того, як у Києві затримали чоловіка, що виклав у TikTok відео з технікою ЗСУ біля ТЦ Retroville. Згодом торговий центр зазнав ракетного удару російських окупантів, внаслідок якого загинуло восьмеро людей. В основі технології Open source intelligence (OSINT) є пошук, аналіз і використання військової, політичної, економічної та іншої інформації з відкритих джерел для прийняття рішень у сфері національної оборони та безпеки, розслідувань тощо. Робота OSINT базується на трьох етапах: збір інформації, чищення даних та аналіз «чистих» даних. Сьогодні штучний інтелект використовують і при розпізнаванні облич окупантів, які вчинили масові вбивства, зокрема в Бучі Київської області, Ізюмі Харківської області тощо. Відкриті дані можуть розповісти багато чого: які моделі підбитої техніки зображено на фото та відео, звідки прилетіли ракети, який населений пункт зафіксовано на фото та відео, як змінюється лінія фронту під час наступу тощо [3].

Відповідно до законодавства про захист інформації ІАС «СОТА» має три контури обробки інформації: загальнодо-

ступний, для службового користування та таємний. Закрита частина стосується лише військової складової. Безпеку обробки даних підтверджено Атестатом відповідності на комплексну систему захисту інформації, виданим за результатами державної експертизи.

В свою чергу, програмні аналітичні модулі ІАС «СОТА» дозволяють забезпечити неупереджений об'єктивний контент-аналіз даних та синхронізацію даних із різних джерел [2]. Завдяки формуванню системи резервних та рухомих ситуаційних центрів, дана роботи може проходити в будь-яких критичних умовах і в будь-якій точці країни.

Національний координаційний центр кібербезпеки при РНБО за підтримки Фонду цивільних досліджень та розвитку США (CRDF Global) та Державного департаменту США вже третій рік поспіль проводить тренінги на теми: «Використання засобів OSINT та ОТ для забезпечення кібербезпеки та протидії дезінформації», «OSINT – розвідка з використанням відкритих джерел» з метою підвищення кваліфікації фахівців державного сектору визначеного Стратегією кібербезпеки України [4].

Наступним кроком опановування основних методик та принципів розвідки з відкритих джерел, інструментів та сервісів, які використовуються для OSINT, з-поміж яких Google-інструменти, пошук по фото, методи деанонімізації в мережі Інтернет, моніторинг соцмереж та месенджерів (телеграм-канали), побудова графіків взаємозв'язків тощо став розроблений фахівцями Інституту постінформаційного суспільства за сприянням ННКЦК при РНБО та Національної академії СБУ навчальний курс для органів сектору безпеки і оборони з імплементації інструментарію Open Source Intelligence (OSINT) у державний сектор [5].

Отже, інформаційно-аналітична система «СОТА» є складною багатошаровою інформаційно-аналітичною системою найвищого рівня захисту інформації, має гнучку, відкриту архітектуру, що дозволяє створювати нові функціональні модулі відповідно до завдань, які виникають при реалізації державної політики в сфері національної безпеки. ІАС «СОТА» є сучасною системою, якою користується вище воєнно-політичне керівництво України для цілодобового спостереження за окремими індикаторами стану національної безпеки України, зокрема моніторинг постачання Україні озброєння від країн-партнерів «від

моменту перетину кордону до розподілу на місцях». Модуль інтегрований з порталом ІАС «СОТА» щодо відслідковування ситуації на лінії бойових дій, моніторингу розміщення сил ворога, ракетних ударів по території України, обстрілів населених пунктів, географічної прив'язки повідомлень, що стосуються воєнних дій, надзвичайних ситуацій та резонансних заяв, у медіапросторі.

Підсумовуючи, слід зазначити, що ІАС «СОТА» Головного ситуаційного центру України при РНБО є сучасним інструментарієм управляння ризиками в галузі національної безпеки та оборони Української держави. Слід також наголосити на необхідності посилення інформаційно-аналітичної діяльності Апарату РНБО в умовах воєнного часу, зокрема, запровадження мобільної компоненти для гарантованого доступу до інформаційних ресурсів та інформаційних систем, функціонування яких забезпечується Апаратом Ради в мирний час і в умовах війни. Важливим моментом також є підвищення кваліфікації фахівців державного сектору із набуття знань з пошуку та аналізу інформації з відкритих джерел (OSINT), а також вмінь захисту власних персональних даних від зловмисних дій ворога.

Література

1. Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони: рішення Ради національної безпеки і оборони України від 4 червня 2021 р., введено в дію Указом Президента України від 18 червня 2021 року № 260/2021. URL: https://zakon.rada.gov.ua/laws/show/n0039525-21#Text.

2. В Апараті РНБО України розроблено та введено в експлуатацію сучасну інформаційно-аналітичну систему «СОТА» (17.11.2021). URL: https://www.rnbo.gov.ua/ua/diialnist/5011.html.

3. Що таке OSINT і як він допоміг викрити вбивства у Бучі (07.04.2022). URL: https://explainer.ua/shho-take-osint-i-yak-vin-dopomig-vikriti-vbivstva-u-buchi/.

4. Понад 2000 держслужбовців з усієї України навчаються використовувати інструменти OSINT (08.02.2023). URL: https://www.rnbo.gov.ua/ua/Diialnist/6089.html.

5. За сприяння НКЦК представники органів сектору безпеки і оборони розпочали навчання з імплементації інструментарію OSINT (26.10.2022). URL: https://www.rnbo.gov.ua/ua/Diialnist/5850.html.

Єманов В. В.
кандидат військових наук,
старший науковий співробітник
Іохов О. Ю.
доктор технічних наук, професор
Споришев К. О.
кандидат технічних наук, доцент,
Національна академія Національної гвардії України

АНАЛІЗ ПРОБЛЕМИ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ВІДКРИТІ ЦИФРОВІ ДЖЕРЕЛА

В умовах широкомасштабного вторгнення РФ особливу небезпеку становить виток критичної інформації через відкриті джерела. З метою визначення масштабності проблеми витоку інформації через відкриті цифрові джерела розглянемо декілька загальнодоступних інструментів, які дозволяють:

Google Lens. Пошук різнотипних даних;

Google maps. Пошук та визначення координат об'єктів що охороняються (військова частина, об'єкти промисловості, енергетики, транспортні вузли та інш.);

InVID-WeVerify. Аналог Google Lens, тільки для відео. Пошук відео, так і його фрагменти через різні пошукові системи;

Primeyes – пошук людей за фото;

SunCalc, Shadowmap – Аналіз тіней на фото, які показують рух сонця в залежності від локації та дозволяють моделювати тіні;

PeakVisor – ідентифікація ландшафту бекграунду фото/ відео. Так, якщо на бекграунді є гори, ця програма допоможе прив'язатись до локації;

Metadata2go – витягує з фото метадані, а 99,9% смартфонів за замовчанням вставляють локацію в фото;

Geolocation Estimaton – нейромережа, яка намагається вгадати локацію за зображенням;

VGG – інструменти для пошуку зображень (від обличчя до коду);

OpenInfraMap – мапа інфраструктурних об'єктів в різних країнах.

Big Data працює, знайти інформацію по відкритих фото/відео/дописах не так вже й важко, як здавалось раніше.

Пошук шляхів вдосконалення методів і способів захисту інформації що розташовується у відкритих джерелах є перспективною задачею сил безпеки та оборони України.

Виникає необхідність створення додаткових органів протидії витоку інформації через відкриті джерела у складі Національної гвардії України.

Іохов О. Ю.
доктор технічних наук, професор
Бєлай С. В.
доктор наук з державного управління, професор
Споришев К. О.
кандидат технічних наук, доцент,
Національна академія Національної гвардії України

НЕЙРОМЕРЕЖІ ЯК ІНСТРУМЕНТ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ В OSINT

За останні десятиліття спостерігається стійкий ріст кількості інформації, що підтверджується результатами дослідження компанії IDC, Cisco. Обсяг «цифрової тіні» – інформації, створюваної про людей автоматично, перевищив обсяг інформації, створюваної людьми самостійно. Створюється й копіюється величезний обсяг цифрової інформації в глобальних масштабах, темпи їх росту носять стрімкий характер. Щомиті сотні мільйонів людей створюють і споживають в онлайн-просторі неуявні обсяги інформації, і простір це фактично не має границь, у рамках яких діяли б національні закони.

Використання інформації у відкритих джерелах, для протидії широкомасштабного вторгнення РФ, значно підвищує ефективність діяльності органів розвідки сил безпеки України. Особлива увага приділяється застосуванню Open Source Intelligence (OSINT).

Основними відкритими цифровими джерелами є фото та відео матеріали. Отримання розвідувальних даних за фотографіями ставить перед фахівцями аналітиками завдання з пошуку та оброблення великого обсягу інформації. Як правило отримання розвідувальних даних проводиться в умовах обмеженого часу.

Під прийняттям рішення розуміється отримання повних даних про об’єкт розвідки.

Метою доповіді є визначення шляхів підвищення якості оброблення великих масивів даних.

Полегшення роботи аналітиків пропонується за рахунок використання програмних інструментів нейромереж. На сьогняшній час нейромережі успішно виконують завдання з пошуку інформації про об’єкти розвідки, розпізнавання особистості порушників. Розробка методів роботи з нейромережами дозволяє зменшити час на отримання розвідувальних даних, підвищити якість отриманих даних, автоматизувати процеси підвищення достовірності інформації. Ці інструменти у загальному підсумку дозволять покращити механізми забезпечення державної безпеки.

В умовах сьогодення, набуває актуальності питання впровадження OSINT в діяльність Національної гвардії України та організації взаємодії з іншими складовими сил безпеки та оборони держави для виявлення загроз національній безпеці.

Фігура В. О.
Національна академія
Державної прикордонної служби України

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ API/PNR ДЛЯ ПРОТИДІЇ ТЕРОРИЗМУ

Протягом 30 років незалежності, наша держава майже постійно стикалася з різного роду загрозами, які були пов’язані як з національною так і прикордонною безпекою. Так, в кінці 2003 року вперше російська федерація розпочала кризу навколо острова Тузла, який розташовується в Керченській протоці. Це відбулося з метою вивчення реакції України та всього цивілізованого світу на зазіхання щодо територіальної цілісності з боку російської федерації, але в той період Україні вдалося відстояти свою територіальну цілісність. Після чого в лютому – березні 2014 року російська федерація розпочала окупацію Криму та з квітня того ж року почала гібридну війнау яка включала не тільки військове захоплення територій але й проведення різного роду терорестичних дій (захоплення частини територій Донецької

та Луганської областей), в результаті чого два обласних цетра: м. Донецьк та м. Луганськ перейшли під повний контроль терорестичних угрупувань: «Донецька народна республіка» та «Луганська народна республіка». Саме після цих подій, керівництвом нашої держави було прийняло рішення як найшвидше удосконалити антитерористичне законодавство та змінити підходи щодо боротьби з даним видом протиправної діяльності, не тільки в середині держави ай безпосередньо на державному кордоні.

Усвідомлення того, що російська федерація по завершенню війни продовжить політику щодо дестабілізації ситуації в нашій країні (не відходячи від своїх імперських амбіцій), змушує нас навіть зараз, в умовах війни, удосконалювати систему національної та прикордонної безпеки.

Так, в 2021 році між Урядом Сполучених Штатів Америки та України було підписано Угоду «Про співробітництво у використанні інформації про тих, хто подорожує». Відповідно до якої було розроблено законопроєкт про ратифікацію даної Угоди, який в даний час перебуває на розгляді у Верховній Раді України (№ 0152 від 20.05.2022). Основною метою даної Угоди являється впровадження в нашій державі системи попередньої інформації про пасажирів (API) та додаткових даних про пасажирів (PNR), яка себе позитивно зарекомендувала в більшості розвинутих країн світу, таких як Канада, Сполучені Штати Америки та більшості країн Європейського Союзу.

Вищезазначена система API/PNR націлена на захист національної та прикордонної безпеки, а також підвищення рівня авіаційної безпеки. Завдяки можливостям даної системи правоохоронні органи та безпосередньо підрозділи Державної прикордонній служби України матимуть можливість виявляти осіб, які загрожують національній безпеці держави, а саме: міжнародних злочинців, терористів, здійснювати більш ефективну протидію торгівлі людьми, виявляти потенційних нелегальних мігрантів та осіб причетних до контрабандної діяльності.

Хочеться звернути увагу, що саме система попередньої інформації про пасажирів (API) з 2013 року до початку війни, успішно функціонувала на базі міжнародного аеропорту «Бориспіль», де вперше була впроваджена Державною прикордонною службою України але наряду з тим, у державі відсутнє законо-

давство, що регулює використання попередніх даних реєстрації особи, що надані авіаперевізником (PNR).

До початку повномасштабної війни, розпочатою російською федерацією 24.02.2022 року, впровадження системи API/PNR планувалося в авіаційних пунктах пропуску через державний кордон України. Проте, у відповідності до вимог Повітряного кодексу України, а також Положення про використання повітряного простору України були вжиті заходи представниками об'єднаної цивільно-військової системи та Державіаслужбою щодо закриття повітряного простору України для всіх цивільних авіа суден з 24.02.2022 року. Отже, по завершенню війни та з відкриттям аеропортів виникне необхідність впровадження системи API/PNR, саме тому необхідно її максимально швидко закріпити на законодавчому рівні.

В Україні вже розпочата робота щодо удосконалення боротьби з тероризмом та різного роду терористичними загрозами, визначено нові суб`єкти, які будуть протидіяти даному виду протиправної діяльності, а також окреслено коло їх повноважень, розроблено механізм взаємодії органів місцевого самоврядування із правоохоронними органами та багато чого іншого.

На сьогоднішній день в нашій державі зареєстрований Проєкт Закону «Про внесення змін до деяких законодавчих актів України щодо вдосконалення боротьби з тероризмом» (№7349 від 05.05.2022 року)[1]. Основним завданням даного законопроєкту являється вдосконалення загальнодержавної боротьби з тероризмом, поліпшення координації та взаємообміну інформації з правоохоронними органами іноземних держав; попереднього виявлення осіб, які є членами або мають відношення до міжнародних терористичних організацій та здійснення своєчасних заходів реагування; забезпечення протидії міжнародному тероризму за допомогою використання бази даних API/PNR, а також міжнародна кооперація з Європолом та Інтерполом.

При розгляді даного законопроєкту пропонується внести зміни в Закон України «Про боротьбу з тероризмом» та до багатьох інших законодавчих актів. Проте, необхідно врахувати, що дані зміни нажаль не в повній мірі узгоджуються з загальнодержавною концепцією створення в Україні системи API/PNR. До прикладу в Чиказькій Конвенції 1944 року (основний міжнаро-

дний документ, який визначає основні принципи роботи міжнародної авіації, Україна приєдналася до даної конвенції в серпні 1992 року) [2] та рекомендаціях Міжнародної організації цивільної авіації щодо записів реєстрації пасажирів (ISBN 978-92-9231-691-4 ICAO 2010) вказано, що держава-учасниця приймає необхідні закони для створення державного механізму використання інформації про пасажирів, необхідної для скорочення термінів здійснення прикордонного контролю, забезпечення необхідного рівня безпеки та дотримання законності. Так, більшістю країн світу з метою можливих загроз національній безпеці, підвищенню рівня авіаційної безпеки, безпеки державного кордону та з метою результативної боротьби з тероризмом, організованою злочинністю, а також ідентифікації та переслідуванні осіб, винних у скоєнні таких злочинів транскордонного характеру було прийнято законодавство, яке регулює питання використання попередньої інформації про пасажирів API/PNR.

Додатково хочеться акцентувати увагу на розпорядженні Кабінету Міністрів України, яке було схвалено 24.07.2019 № 687-р «Про Схвалення стратегії інтегрованого управління кордонами на період до 2025 року» [3]. В якій зазначено, що Адміністрація Державної прикордонної служби України спільно з іншими органами виконавчої влади повинна розробити Закон України, який буде регулювати наступні питання: в якому форматі і в які терміни авіаперевізник буде надавати попередню інформацію про пасажирів API/PNR, а також відповідальність яку будуть нести авіаперевізники за не подання або не своєчасне подання даної інформації. Отже, в законопроєкті № 7349 не до кінця врегульовані вищеперераховані питання, а також він не містить державницького підходу, щодо захисту персональних даних осіб, їх узагальнення та обробку, зобов`язань, які Україна взяла в рамках міжнародних угод та договорів. Оскільки, впровадження бази даних API/PNR початково планувалося безпосередньо на державному кордоні України (в авіаційних пунктах пропуску), що б дозволило не лише ефективно протидіяти терористичній загрозі, ай надало б можливість виявляти потенційних нелегальних мігрантів, міжнародних злочинців, осіб причетних до торгівлі людьми та контрабандної діяльності, а також запобігти багатьом іншим злочинам, які носять транснаціональний характер.

Саме тому виникає потреба надання ширших повноважень та доступу до вищезазначеної бази підрозділам Державної прикордонної служби України.

Література

1. Про внесення змін до деяких законодавчих актів України щодо вдосконалення боротьби з тероризмом : проєкт Закону України від 05 травня 2022 р. № 7349. URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1288565 (дата звернення: 19.03.2011).

2. Конвенція про міжнародну цивільну авіацію 1944 р. URL: http://zakon5.rada.gov.ua/laws/show/995%20038 (дата звернення: 20.03.2011).

3. Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 року : розпорядження Кабінету Міністрів України від 24 липня 2019 р. № 687-р. URL: https://zakon.rada.gov.ua/laws/show/687-2019-%D1%80#Text (дата звернення: 21.03.2011).

РЕКОМЕНДАЦІЇ
круглого столу «Актуальні питання використання методів і засобів OSINT у роботі підрозділів захисту національної державності»

Під час проведення активної фази відбиття агресії рф проти нашої держави важливим компонентом забезпечення перемоги стало використання результатів здійснення розвідки на основі відкритих джерел *(англ. Open Source Intelligence, OSINT).*

Учасники круглого столу дійшли висновку, що первинна інформація з відкритих джерел після її аналітико-синтетичної переробки може стати цінними знаннями, які використовуватимуться для ефективної протидії військовій агресії рф проти нашої держави. Тому необхідно залучати якомога більше можливостей здобування інформації стосовно ворога та його пособників як в Україні, так і за її межами, з урахуванням потенціалу електронних мереж, державних, галузевих та корпоративних баз даних, інших відкритих джерел тощо.

При цьому надзвичайно важливу роль у наближенні перемоги відіграє співпраця Служби безпеки України з державними та правоохоронними органами, військовими формуваннями, громадськими об'єднаннями та дослідниками у цій сфері з отримання актуальної інформації, яка використовується для ураження ворожих військ, виявлення шпигунів, колаборантів та осіб, які вчинили злочини проти України та її громадян, формування доказової бази для притягнення до відповідальності винних у вчиненні геноциду та військових злочинів.

Учасники круглого столу наголосили, що діджиталізація процесів здобування інформації стала ефективним інструментом протидії агресору, проте необхідність звільнення окупованих територій, забезпечення досягнення переможних результатів активної фази бойових дій та притягнення до відповідальності ініціаторів та безпосередніх виконавців злочинних дій спонукає до пошуків нових форм, методів та засобів здобування інформації з відкритих джерел, поглиблення міжнародної співпраці дослідників, ефективного використання отриманих даних для забезпечення перемоги України. У зв'язку з цим, на круглому столі розроблені такі **рекомендації**:

– продовжити практику моніторингу загроз національній державності України за допомогою методик, технологій та інструментів OSINT;

– розширити спектр питань, що підлягають вивченню із застосуванням методів OSINT, – не тільки для збору та узагальнення інформації про факти і ознаки злочинів у сфері національної безпеки, осіб, причетних до таких видів злочинів, а й для розробки критеріїв оцінки соціально-політичної, економічної та інших сфер суспільного життя щодо попередження виникнення передумов кризових явищ у суспільстві, загроз державній безпеці тощо;

– проаналізувати досвід використання методів і засобів OSINT спецслужбами країн-союзників України в інтересах розвіддіяльності;

– опрацювати можливість адаптації стандартів НАТО з використання OSINT для сектору безпеки України;

– продовжити взаємодію громадянського суспільства та сектору безпеки і оборони України у сфері отримання інформації з відкритих джерел інформації, напрацювати правові механізми такої співпраці та унормувати їх;

– розробити правові механізми регулювання збору, аналізу інформації з відкритих джерел з метою використання в оперативній практиці під час документування злочинів проти державної безпеки України;

– дослідити перспективи використання методів і засобів OSINT для фіксації злочинів військовослужбовців рф на території нашої держави;

– здійснити дослідження потенціалу застосування нейромереж для здобування інформації з відкритих джерел в інтересах державної безпеки і оборони України;

– зосередити зусилля на створенні ефективних правових та технічних засобів захисту інформації з метою недопущення використання її ворогом на шкоду національній безпеці України;

– розглянути можливість ширшого використання цифрової криміналістики у доказуванні фактів вчинення воєнних та інших злочинів проти національної безпеки України;

– опрацювати напрямки структуризації контенту для спрощення пошуку інформації у web-середовищі;

– звернути увагу дослідників на можливість виявлення за допомогою методів і засобів OSINT осіб, схильних до співпраці з ворогом;

– розширити практику використання даних інформаційно-аналітичної системи «СОТА» як інструменту аналізу та управління ризиками у сфері національної безпеки і оборони України;

– розширити можливості застосування API\PNR для протидії терористичній діяльності;

– опрацювати питання щодо використання чат-боту штучного інтелекту ChatGPT для потреб OSINT-досліджень.

ЗМІСТ

Наукове видання

АКТУАЛЬНІ ПИТАННЯ ВИКОРИСТАННЯ МЕТОДІВ І ЗАСОБІВ OSINT У РОБОТІ ПІДРОЗДІЛІВ ЗАХИСТУ НАЦІОНАЛЬНОЇ ДЕРЖАВНОСТІ

Збірник матеріалів круглого столу
(м. Київ, 31 березня 2023 року)

Частина 1

Друкується в авторській редакції

Технічне редагування *Т. О. Коркач*

Формат 60х84/16. Ум. друк. арк. 4,75.
Обл.-вид. арк. 3,55. Тираж 10 прим. Наряд №

Реєстр. № 29/2/1/1-455/ві від 5 червня 2023 р.

Видавець і виготовлювач
Національна академія Служби безпеки України,
03022, м. Київ, вул. Михайла Максимовича, буд. 22
Свідоцтво суб'єкта видавничої справи ДК № 6844 від 17.07.2019.