Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Розвідка відкритих джерел інформації для виявлення загроз безпеки бізнесу

Виконала:
студентка VI курсу, групи СБм-61
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) *Николин К. П.* (прізвище та ініціали)

Керівник (підпис) *Александер М. Б.* (прізвище та ініціали)

Нормоконтроль (підпис) *Лобур Т.Б.* (прізвище та ініціали)

Завідувач кафедри (підпис) *Загородна Н.В.* (прізвище та ініціали)

Рецензент (підпис) Михалик (прізвище та ініціали)

Тернопіль
2022

АНОТАЦІЯ

Розвідка відкритих джерел інформації для виявлення загроз безпеки бізнесу // Кваліфікаційна робота освітнього рівня «Магістр» // Николин Катерина Петрівна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2022 // С. 72, рис. – 18, табл. – 1, додат. – 1, бібліогр. – 49.

Ключові слова: OSINT, OPEN SOURCE INFORMATION, БЕЗПЕКА, ІНФОРМАЦІЯ, РОЗВІДКА, ДОСТУП.

Кваліфікаційна робота присвячена дослідженню застосування технології OSINT для виявлення загроз безпеки бізнесу.

У першому розділі проводиться опис основних понять розвідки з відкритих джерел, загальнодоступної інформації; також наводиться опис переваг й недоліків застосування OSINT. Проводиться огляд й характеристика основних дисциплін збору розвідданих.

У другому розділі розглядаються основні тактики збору інформації з відкритих джерел OSINT, досліджуються інструменти збору інформації, описуються принципи їх роботи.

У третьому розділі проводиться практичне застосування OSINT-технологій для перевірки витоків даних цільової компанії, та проводиться аналіз ризиків безпеки компанії.

ANNOTATION

Open Source Intelligence for Business Security Threats Identification // Qualification paper of the educational level “Master” // Kateryna Nykolyn // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, СБм-61 group // Ternopil, 2022 // P. 72, fig. - 18, tables - 1, annexes - 1, references - 49.

Key words: OSINT, Open Source Information, security, information, intelligence, access.

The qualification work is devoted to the study of the application of OSINT technology to identify business security threats.

The first section describes the basic concepts of Open Source Intelligence, publicly available information; also the secrion describes the advantages and disadvantages of using OSINT. The main intelligence gathering disciplines are reviewed and characterized.

In the second section, the main tactics of collecting information from open OSINT sources are considered, the tools for collecting information are studied, and the principles of their work are described.

In the third section, the practical application of OSINT technologies is carried out to check the data leakage of the target company, and the analysis of the company's security risks is carried out.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ACOUSTINT - Acoustical intelligence

AP - Access point

AS - Autonomous System

BEC - Business email compromise

CIDR - Classless Inter-Domain Routing

CLI - Command-line interface

COMINT - Communications intelligence

CVE - Common Vulnerabilities and Exposures

ELINT - Electronic intelligence

FISINT - Foreign instrumentation signals intelligence

GEOINT - Geospatial Intelligence

GPS - Global Positioning System

HUMINT - Human Intelligence

ICD - Intelligence Community Directive

IDS - Intrusion Detection System

IMINT - Imagery Intelligence

IP - Internet Protocol

IPS - intrusion prevention system

IRINT - Infrared intelligence

KYC - Know Your Customer

MASINT - Measurement and Signature Intelligence

MX - Mail exchanger

NUCINT - Nuclear intelligence

OSINF - Open source information

OSINT - Open-Source Intelligence

PII - Personally identifiable information

PSK - Pre-Shared Key

RADINT - Radar Intelligence

SIGINT - Signals Intelligence

SIM - Subscriber Identity Module

SMTP - Simple Mail Transfer Protocol

SOCMINT - Social media intelligence

SSN - Social Security number

TELINT - Telemetry intelligence

TOR - The Onion Router

URL - Uniform Resource Locator

VPN - Virtual private network

WEP - Wired Equivalent Privacy

WPA - Wi-Fi Protected Access

БД - База даних

ЗМІ – Засоби масової інформації

ОС - Операційна система

ПЗ - Програмне забезпечення

ЦРУ – Центральне розвідувальне управлін

ЗМІСТ

ВСТУП

Актуальність теми. Організації як у державному, так і в приватному секторі приділяють все більше уваги відкритим джерелам даних при проведенні операцій зі збору розвідувальної інформації. Розвідка з відкритих джерел (OSINT) - це структурований підхід до вилучення значущої інформації з відкритих даних, який передбачає каталогізацію, сортування і визначення пріоритетів даних в рамках розвідувальної діяльності. У 2022 році OSINT став важливим інструментом для забезпечення кібербезпеки в багатьох галузях промисловості. Одними з найбільших користувачів розвідки з відкритих джерел зараз є також міжнародні організації (ООН та Червоний Хрест), правоохоронні органи, і звичайно бізнес.

Мета і задачі дослідження. Метою даної кваліфікаційної роботи освітнього рівня «Магістр» є ідентифікація ризиків, пов’язаних з безпекою бізнесу у цифровому просторі, шляхом застосування OSINT-технологій, що дозволить провести оцінку захищеності організації від витоків даних й інших загроз, забезпечивши своєчасну реакцію на такі загрози.

Задля досягнення поставленої мети постає необхідність у виконанні наступних завдань:

- розглянути тактики й етапи проведення OSINT;
- розглянути нормативно-правове регулювання OSINT;
- розглянути інструменти OSINT-розвідки та їх застосування;
- сформулювати особливості проведення OSINT-розвідки для бізнесу;
- провести експериментальну OSINT-розвідку для цільової бізнес-організації;
- оцінити ризики загроз бізнесу на основі отриманих розвідданих.

Об’єкт дослідження. Основні загрози безпеки бізнесу.

Предмет дослідження. Технології OSINT розвідки для бізнесу.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає у тому, що сформульовано особливості проведення OSINT розвідки для бізнесу та

проведено дослідження витоків інформації цільових об’єктів приватної компанії, що дозволяє ідентифікувати існуючі загрози.

Практичне значення одержаних результатів. Описаний цикл проведення ефективного OSINT-розслідування, основні тактики, які слід застосовувати під час проведення розвідки; проведено розвідку з відкритих джерел для цілі, що допоможе виявити потенційні ризики і загрози для системи корпорації.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на: X науково-технічній конференції «Інформаційні моделі, системи та технології» (м.Тернопіль, 2022).

Публікації. Основні результати кваліфікаційної роботи опубліковано у праці конференції (див. Додаток А).

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ МЕТОДОЛОГІЙ РОЗВІДКИ НА ОСНОВІ ВІДКРИТИХ ДЖЕРЕЛ

1.1 Поняття дисципліни OSINT

1.1.1 Головні аспекти OSINT

Сьогодні смартфони, мережа Інтернет, соціальні мережі та аналітика даних сприяють величезному викриттю й поширенню даних критичної важливості про різного типу події, таким чином провокуючи витоки інформації, розповсюдження новин і навіть секретів.

Розвідкою в широкому розумінні можна вважати практику методичного збору, аналізу інформації критично важливого характеру, із метою отримання певних переваг та, звичайно, забезпечення безпеки. Розвідка постає як синонім до слів «шпигунство», «таємні операції», водночас здебільшого зосереджуючись на інформації, яка перебуває ззовні, здійснюючи її методичний збір, обробку, аналіз даних – як вже відомих, так і тих, що перебувають за периметром; розвідка не базується на добуванні інформації через крадіжку за допомогою таємних методів.

З часом під терміном «розвідка» набув значення методичного збору інформації, яка має певну цінність, зацікавленими особами, що приймають рішення; вона може стосуватися внутрішніх справ країни й іноземних держав, загальних глобальних інцидентів [1].

OSINT (англ. Open-Source Intelligence), або розвідка з відкритих джерел – це технології і методології збору, добування із загальнодоступних джерел дієвих розвідданих із метою використання, маніпуляцій і поширення, щоб задовільнити певні розвідувальні потреби; при цьому не допускається порушення законів. Зараз OSINT головним чином використовується правоохоронними органами для забезпечення функцій національної безпеки, а також діловою розвідкою, аналітиками [2]. Відомо, що основна частина розвідданих, за деякими джерелами - до 80 відсотків, отримується із саме загальнодоступних джерел, що підтверджує

факт можливості поширення специфічних розвідданих по периметру, відмінному від традиційного загальноприйнятого розвідувального середовища.

Витоки OSINT пов'язують із Уільямом Донованом: під час Другої світової війни він створив Управління стратегічних служб, яке з часом перетворилося на Центральне розвідувальне управління – ЦРУ – служба зовнішньої розвідки Сполучених Штатів Америки [1]. Один із робочих відділів спеціалізувався на зборі, систематизації й аналізі інформації з безлічі загальнодоступної інформації. OSINT сьогодення можна трактувати як конвергенцію технологій, підсумовуючи його історію. Нові методи будуть й надалі осучаснювати розвідку з відкритих джерел і її тактики; завдяки технологіям штучного інтелекту техніки OSINT змінюються, що робить цю сферу все більш привабливою для інвестування [6].

Серед позитивних характеристик інформації, що позиціонується як загальнодоступна, можна виділити різноманітність тематики наповнення, низьку вартість при зборі, оперативність, легку доступність, етичну складову; проте варто зазначити й негативні характеристики: присутність певного потенціалу виникнення дезінформації, фрагментарність правди, суперечливість [3]. Обрисування як позитивних, так і негативних характеристик загальнодоступної інформації є еквівалентно важливо. Беручи до уваги те, що публічна мережа є досить зручним і таким, що не потребує багато зусиль майданчиком для розповсюдження думок і, відповідно, впливу, різні суб'єкти намагаються модифікувати інформацію, а це ускладнює її аналіз та оцінку [3].

Виділяють низку відкритих джерел OSINT, які нерідко перетинаються:

- Засоби масової інформації: всесвітнє телебачення, газети й журнали в друкованому, і не тільки, вигляді, радіо. Такий вміст ідентифікує себе як журналістика. Новинні засоби масової інформації (ЗМІ) включають у себе сайти, «агрегатори» новин, містять також зміст, вироблений державою, за умови його умисно влаштованого просування ЗМІ.
- Мережа Інтернет: найбільш широка й легкодоступна категорія, що включає соціальні мережі Twitter, Facebook, Instagram та ін., YouTube, блоги користувачів, що містять відеоматеріали й інші медіа матеріали;

- Публічні урядові (державні) дані: представлені онлайн чи в друкованому вигляді матеріали прес-конференцій, бюджетні й урядові звіти, промови;
- Академічні публікації: наукові журнали, дисертації, наукові роботи, тези, матеріали симпозіумів і професійних асоціацій;
- Дані комерційного характеру: бази даних, різноманітні комерційні медіа файли, фінансові оцінки і т. п.;
- Так звана «сіра» література: огляди ринків, дискусійні й робочі документи, науково-технічні звіти, звіти про відрядження, неофіційні урядові матеріали, препринти й інше [4, 5]. Основні припущення постають у тому, що існує певна інституційна присутність й згуртованість, і більша частина такого вмісту існує не лише в онлайн-просторі. «Сіра» література потрапляє в ужиток не так швидко й масово, використовується не надто систематично [7].

Сьогодні розвідка на основі відкритих джерел застосовується не тільки в розвідувальному середовищі, а й у наступних сферах:

- Журналістика;
- Правоохоронні структури;
- Рекрутинг;
- Тестування на проникнення;
- Агентурна розвідка й соціальна інженерія;
- Цивільний захист;
- Захист бізнесу;
- Пошуки зниклих безвісти, порятунок людей;
- Громадський розшук;
- Управління кіберризиками [1].

1.1.2 Аналітичний огляд переваг й недоліків OSINT

Необхідно зазначити, що користь зібраної інформації з допомогою OSINT значно перевищує негативні сторони цього методу. Нижче будуть наведені зібрані позитивні аспекти дисципліни збору даних з відкритих джерел:

- Велика кількість інформації збирається із значною швидкістю: жодна розвідувальна технологія не має властивості за короткий час проводити пошук через відкриті джерела значного обсягу інформації; велику кількість інформації можна генерувати з допомогою саме цифрових даних;
- Отримання інформації відбувається у простий спосіб: відкриті джерела «віддають» наявну інформацію значно легшим способом завдяки суттєвому розвитку технологій і всесвітньої мережі Інтернет. Фактично для заволодіння інформацією з відкритих джерел достатньо смартфона чи іншого пристрою з відкритим доступом в Інтернет;
- Низька вартість збору інформації з відкритих джерел: зазвичай загальнодоступними є дані з відкритих джерел, тож переважно вони є й безкоштовними. Проте це не відміняє того факту, що існує множина певних комерційних продуктів, таких як наукові статті й видання, журнали, доступ до яких надається після відповідної сплати коштів.
- Збір інформації охоплює широкі спектри змістовних одиниць: значна перевага пошуку у відкритих джерелах полягає в тому, що при цьому охоплюються безліч тем, до прикладу, національна безпека. При застосуванні відмінних методологій збору інформації чи виконання прихованого пошуку через одне людське джерело така перевага не працюватиме.
- Інформація є доступною на різних мовах світу: вміст іноземних веб-сайтів завжди можна перекласти на більшість мов завдяки технології машинного перекладу.
- Інформацію можна шукати в режимі реального часу: OSINT дозволяє відстежувати, наприклад, локалізації спалаху епідемії, маршрути мігрантів, слідкувати за наслідками терористичного акту, чи навіть переглядати демонстрації насильницьких актів – усе це в режимі реального часу.
- Можливість перевірити на справжність, автентифікувати секретну інформацію: цінним є можливість спостерігати й відслідковувати, чи не розповсюджуються певні конфіденційні дані відкритими джерелами. Це дозволяє направити у потрібне русло збір секретних даних у майбутньому.

- Збір інформації недавнього часу: OSINT ефективно застосовуваний за потреби реконструкції подій минулого й збору ширшого масиву інформації щодо цих подій.

- Пошук інформації в одному місці: процедура збору й отримання даних не передбачає зміни локації – міста, країни.

- Ефективність для бізнес-аналітики: застосування OSINT допомагає, наприклад, досліджувати ринок, проводити оцінку конкурентів, планування й рекламу власних бізнес-проектів; прийняття ефективних бізнес рішень;

- Відносно низький рівень небезпеки: спосіб збору інформації на основі відкритих джерел можна охарактеризувати як спосіб з низькими ризиками, тому цей підхід є прийнятним із перспективи безпеки. Це дозволяє зокрема не використовувати інші джерела, наприклад, людські, для збору інформації, або ж значно зменшити застосування інших методів, таким чином оптимізувавши їх використання.

Негативні аспекти збору даних на основі відкритих джерел не перевищують користі цього методу, проте також мають місце:

- Загальнодоступна інформація може мати маніпулятивний характер: ефективно впливати у потрібному руслі можна на масив суспільних знань, поширюючи різну інформацію, зокрема дезінформацію. Тому будь-який зібраний матеріал має бути перевірений у кілька етапів.

- Величезна кількість інформації у відкритому доступі: щодень кількість інформації розповсюджується з величезною швидкістю, що може провокувати виникнення заплутаності й складності у фільтрації потрібної інформації.

- Виникнення протиріч в інформації: це зумовлено демократизацією мережі й можливостями досить легкого поширення користувачами інформації. Це створює складнощі й необхідність оптимізувати розвідувальні дані до прийнятного рівня точності [3].

1.2 Моделювання етапів OSINT-розслідування

Необроблені дані компілюються у розвідувальну інформацію за спеціальним циклом розвідки, аби така інформація могла в подальшому бути застосована задля досягання певних бізнес-цілей. Такий процес є циклічним за своєю природою, а отже має прямий вплив на визначення майбутніх траєкторій розслідування [13].

Різноманітні джерела пропонують кілька варіантів формалізації процесу розслідування OSINT, різні концептуалізації циклу розвідки включають переважно 4 – 7 етапів, при цьому всі концепції індивідуально групують етапи в окремі візуалізації, описуючи оди і той самий процес. Концептуалізація процесів проходить для різних організацій здебільшого в індивідуальному порядку. Розвідувальний цикл можна окреслити як структурований процес, що описує кроки, які ґрунтуються на зборі розвідувальної інформації. Така інформація з присвоєною їй вартістю (розвіддані) – це вивід циклу розвідування, у якому у свою чергу необроблена інформація потрапляє в цикл і виходить з нього, отримуючи певну цінність для компанії [11][1].

Збільшення в кількості дезінформації, що впроваджується щоденно у величезну мережу, робить збір розвідданих усе більш складним і ресурсомістким процесом [12]. Розвідувальний цикл під час керування розслідуваннями в Інтернеті має відігравати значну роль. Такий цикл за допомогою інформації із відкритих джерел (англ. OSINF) створює розвідку на основі відкритих джерел, забезпечуючи розподілення цих розвідданих серед відповідних впливових сторін. OSINT-аналітик повинен мати на увазі, що релевантною можна кваліфікувати тільки певну частку OSINF, лише долю ефективної, актуальної і релевантної інформації. У свою чергу, ресурсомістким і таким, що вимагає значних зусиль, є процес оцінки релевантності даних; такі дії зосереджуються по цілому спектру розвідувальних даних. Для максимально надійного звітування потрібне повне забезпечення контексту, для цього велику роль відіграють кроки, які передбачає перетворення даних із необроблених розвідувальних даних.

У найбільш простий спосіб етапи процесу OSINT можна описати як отримання інформації, аналіз і перевірка цих даних, оцінка цінності даних, передача інформації зацікавленим особам (наприклад, клієнту). Етапи процесу OSINT розслідування детально наведені у наступних параграфах:

1. Спрямування. На цьому етапі відбувається підготовка до фактичного розслідування, коли виникла потреба у вигляді запиту клієнта; при цьому має бути присутнє чітко поставлене завдання й вимоги до розвідданих. Постають зазвичай наступні завдання: виконати оцінку загроз подій чи осіб, отримати цільові профілі, ідентифікувати облікові записи і їх атрибуцію. IT-безпека компанії постановляє такі завдання, які здебільшого зосереджуються на вирішенні потреби оцінити загрози системи чи цифрового сліду компанії. Цей етап передбачає створення аналітиком плану збору розвідданих, де повинні бути чітко розплановані зусилля збору й визначені пріоритети розвідувального продукту. Як додаток, аналітик складає письмовий план процесу збору, із допомогою якого він викриє можливу проблемну область. Аналітик окреслює у майбутньому ним досліджувані джерела інформації, методи збору даних; необхідним є обізнаність про актуальні джерела, адже деякі нові платформи з'являються й популяризуються досить швидко. При застосуванні автоматизованих систем збір може базуватися й на пошукових термінах [11].

2. Збір. Цей етап починається після чіткого визначення вимог до інформації в плані збору; метою цього етапу є забезпечення цінності, точності й релевантності інформації. Ідея етапу криється у тому, щоб здійснюючи систематичний пошук публічної інформації й використовуючи отримані референтні ідентифікатори, пов'язувати знайдену інформацію, щоб отримати результат. При зборі можна використовувати можливості пошукових інструментів, сервісів, які передбачають оплату за їх застосування; здійснювати веб-пошук ідентифікаторів (імена, адреси електронної пошти, доменні імена, номера телефонів і т. п.). Тобто кожен крок робочого процесу має починатися з ідентифікатора і мати свої шляхи пошуку й відповідно конкретні інструменти. Після отримання деяких даних, наприклад, імені користувача, можна підібрати

комбінацію для адреси електронної пошти, пов’язаної із цим користувачем; потім вхідні дані можна перевірити на наявність у БД, що містять скомпрометовану інформацію. Тож цей етап передбачає кілька підходів, застосування різних пошукових систем; укінці отримані результати фіксуються. Збір даних може бути здійснений із різнотипних джерел, наприклад: відкриті демографічні дані, судові справи, реєстри злочинців, документи на транспортні засоби, телефонні довідники, витоки даних, темна павутина, журнали, статті та ін. [1].

3. Обробка. У широкому розумінні етап обробки можна описати як перетворення даних, що були зібрані, у інформацію. Це передбачає розшифрування, переклад даних у потрібний зрозумілий формат; перевірка інформації на придатність використання. Етап обробки може передбачати не лише переклад тексту на потрібну мову, а й обробку фото й відеоматеріалів таким чином, щоб зробити їх форми придатними формами розвідданих. Зараз безліч програмних засобів полегшують етап обробки таким чином, щоб задачі виконувалися більш ефективно й швидко [7].

4. Аналіз. Цей етап започатковується на вихідних даних попереднього: після збору, обробки та оцінки інформації. Аналіз ґрунтується на ідентифікації невідповідностей, певних тенденцій чи закономірностей шляхом об’єднання інформації. Це надає можливість аналітикам формувати звіти, практичні розвіддані клієнтам чи зацікавленим особам, щоб ті могли використовувати отриману інформацію для роботи з інцидентами. Виділити важливість інформації і зробити загалом аналітичні висновки допомагає контекстуальна інформація на стадії аналізу. Окреслити важливість інформації дозволяє зрозуміти, чи трапився певний інцидент, чому він трапився, чи корелюється він із раніше відомими фактами і чи є актуальним, які наслідки може мати в майбутньому. Аналітик формує SMART-рекомендації на основі зібраних даних, орієнтовані на результат. Вони повинні бути сформовані таким чином, щоб враховувалися імовірні заходи реагування, їх вартість і потенційні ризики, потрібний результат, вигоди від цих заходів, економічну ефективність.

5. Поширення інформації. Цей етап передбачає поширення клієнтам кінцевого продукту, у потрібному форматі. Розвіддані слід доводити клієнту з виділенням ключових аспектів, фактів й із зазначенням рекомендацій. Продуктами OSINT можуть слугувати дані у вигляді звітів, резюме, офіційних презентацій, усних брифінгів, геопросторових карт та ін., тобто у необхідному для цільової аудиторії форматі. Аналітик також може підготувати звіт у різних форматах одночасно.

6. Зворотній зв'язок. Цей етап передбачає оцінку кінцевого продукту, який був поширений, перевірку, чи задовольняє він усі аспекти, визначені на початку. Така оцінка продукту може слугувати для оптимізації чи коригування подальших продуктів [11] [14].

1.3 Огляд інших дисциплін збору розвідданих

Насправді OSINT постає лише як одна з технологій збору розвідувальної інформації. Усталеного списку дисциплін збору розвідувальної інформації не існує, проте у розвідувальному товаристві Сполучених Штатів Америки панує консенсус щодо наступних п'яти дисциплін:

- Власне OSINT. Розвідка на основі відкритих джерел інформації отримується законними методами з широкого діапазону форматів джерел на базі загальнодоступної інформації. При цьому, існує так званий SOCMINT - розвідка соціальних мереж, він може застосовуватися задля моніторингу вмісту соціальних мереж (Instagram, Facebook). SOCMINT головним чином можна вважати піддисципліною розвідки на основі відкритих джерел OSINT [8].
- HUMINT (англ. Human Intelligence). Цей тип розвідки визначається як агентурна розвідка, коли добувається інформація таких характерів, як воєнний, політичний, науково-технічний, військовий; для такої цілі задіюються спеціально завербовані особи (агенти), розвідники під прикриттям. Основна мета такої розвідки полягає у тому, щоб заволодіти секретними відомостями, документами, які іншим підходом зібрати зазвичай неможливо [9]. HUMINT – одна з найстаріших

дисциплін збору розвідувальної інформації, ставши у двадцятому столітті головним інструментом збору даних урядів, аж до кінця століття [8].

- SIGINT (англ. Signals Intelligence), або розвідка сигналів, виник у 1850-их роках, і відбувається через перехоплення сигналів супротивника і їх обробку, виконуючись із різних платформ – наземні об’єкти, літаки, кораблі. Цей тип розвідки завдячує головним чином винайденню телеграфії. При цьому зашифровуються й неворожі повідомлення задля неможливості противником перехопити їх. При SIGINT здійснюється підключення до каналів передавання сигналів і до мереж зв’язку, щоб перехопити електронні комунікації ворога, виконання шифрування-дешифрування повідомлень. У свою чергу, SIGINT теоретично ділиться на три піддисципліни: комунікаційна розвідка (англ. COMINT), що націлюється на трафік телепринтерів і азбуку Морзе, і на текстові й голосові повідомлення різних форматів, головним чином відбувається перехоплення комунікацій із подальшою передачею від пристрою до пристрою і задіянням криптографічних методів; електронна розвідка (англ. ELINT) перехоплює й безпосередньо аналізує некомунікаційні передачі, які здійснюються з допомогою радарів чи іншого електромагнітного випромінювання, при цьому в обороті зазвичай виключно інструменти, які є майном урядів, тому тут має місце висока засекреченість і захищеність; розвідка сигналів іноземних приладів (англ. FISINT) передбачає перехоплювання телеметрії космічних апаратів чи систем озброєння, а видобуті розвіддані надають можливість проаналізувати, виділивши основні характеристики цих пристроїв і систем.

- GEOINT (англ. Geospatial Intelligence) трактується як геопросторова розвідка і ґрунтується на об’єднуванні розвідувальних даних геопросторової інформації і знімків. Ця дисципліна забезпечує моніторинг людської діяльності, прив’язаний до певної географічної місцевості і її умов, шляхом аналізу зображень - частотного, часового і статичного. GEOINT застосовується як у військових цілях, так і в інших, не пов’язаних із воєнною діяльністю. Як піддисципліну геопросторової розвідки можна трактувати видову розвідку IMINT (англ. Imagery Intelligence), де дані видобуваються із джерел інфрачервоного випромінювання,

лазерів, радіолокаційних датчиків, візуальних і супутникових фотографій. Зараз значно збільшилась кількість космічних апаратів зйомки, і відповідно усе більшому числу урядів різних країн стають доступні такі розвіддані; водночас питання якості залишається актуальним, її підвищенню сприятиме боротьба з наслідками несприятливих природних явищ шляхом задіяння високорозвинених технологій. Можна виділити такі комерційні рішення, що пропонують надання знімків високої роздільної здатності: Terra Bella, Orthecast, Planet Labs, BlackSky Global, XpressSAR; таким чином деякі недержавні суб'єкти, організації гуманітарного напрямку й бізнеси в цілому мають перевагу імплементовувати GEOINT.

- MASINT (англ. Measurement and Signature Intelligence), або вимірювально-сигнатурна розвідка, є загальним терміном, що застосовується для визначення спектру засобів високотехнологічного виявлення для виміру різних типів сигнатур (біологічних, хімічних, радіочастотних, акустичних, радіаційних, інфрачервоних, спектроскопічних). При MASINT використовуються технології дистанційного зондування задля збору даних просторових, метричних, модульних, кутових. Вимірювально-сигнатурна розвідка дозволяє ідентифіковувати такі інформаційні патерни, які є перебувають у використанні в інших системах. До MASINT прив'язують наступні п'ять піддисциплін (джерел): TELINT - телеметрична розвідка, RADINT - радіолокаційна розвідка, NUCINT - ядерна розвідка, IRINT - інфрачервона розвідка, та ACOUSTINT - акустична розвідка. У досить широкому полі інформаційних середовищ зараз задіюється MASINT: для виявлення літаків й безпілотників, ракет, оцінки природних ресурсів, ліквідації небажаних наслідків від стихійних лих, моніторингу й контролю надання допомоги біженцям [10].

1.4 Вплив OSINT на міжнародну безпеку

Широка дискусія щодо OSINT пов'язана з тим, як змінюють сучасні технології природу державної таємниці і ту роль, яку відіграє засекречення у державному управлінні. У цьому питання повинна бути встановлена рівновага. Із

одного боку, комунікація через Інтернет збільшує рівні свобод від окремих осіб до значних соціальних сил і формувань, а з іншого – дає можливість державам їх придушувати. Із перспективи держави OSINT призводить до двох результатів. Короткостроковим наслідком стає перегляд розвідувальної і військової політик, щоб запобігти витоку інформації через використання таких засобів комунікації. Це включає внесення простих корективів поведінки, таких як застосування смартфонів, присутності у соціальних мережах, а також перехід на нові варіанти способів шифрування і зберігання важливих політичних секретів. Довгострокова перспектива передбачає активне використовування особами можливостей OSINT, що призводить до викриття деяких таємниць державного характеру, як результат це може повпливати на позиції держав під час надзвичайних ситуацій, криз. Уряди як авторитарні, так і демократичні здійснюють спроби відстояти власні версії подій, проте усе складніше доведеться встановлювати на це монополію. Така ситуація може стати рушійною силою для урядів для блокування й придушення громадських механізмів альтернативної інформації, щоб вносити корективи у те, як застосовується секретність у державному управлінні.

Проте не існує підтвердження того, що така масова аналітика OSINT впливатиме так само на всі держави. Більше того, OSINT не зможе сприяти зменшенню опору на секретність державами. Цифровий OSINT може спричинити появу так званої «асиметрії секретності» між тими урядами, які з високою толерантністю ставляться до витрат на аудиторію (автократії), і між тими, що є чутливішими до них (демократії). Викриття й витоки громадян можуть компенсуватися через внутрішні засоби репресій – цензура, арешти, тому в широкому значенні автократії вважатимуть цифровий OSINT неактуальним.

Із перспективи довгостроковості соціальні медіа-платформи й глобальна мережа повинні перейти до ділової рівноваги, коли уряд матиме перевагу в плані контролю інформації, або шляхом контролю великих технологічних організацій, чи через укладання домовленості про розподілення повноважень, де будуть чітко визначені юрисдикційні зони для мінімізації витоків даних.

Із цією метою при OSINT усе популярнішим стає шлях зосереджування зусиль на тих аспектах, які зможуть привернути увагу місцевості у більш широких питаннях і зможуть водночас надати певний політичний імпульс.

Термін секретності не зникає, але дещо модифікується через рух відкритих інформаційних полів; факти, події, які раніше можна було вважати таємними, сьогодні втратили свій статус. Закономірно наростає необхідність перебудови мислення щодо того, яку інформацію варто розкривати в мережі, а яку ні, і як поводитися, коли таємниці таки відкриваються. Поки уряди не адаптуються до новітніх комунікаційних платформ та витоків інформації, розмитим поняттям поставатиме секретність, і надаватиме вплив на всі сторони дебатів між державою і суспільством [10].

1.5 Висновки до першого розділу

У ході написання першого розділу було чітко розкрито поняття розвідки на основі відкритих джерел OSINT, було описано, що являє собою інформація із загальнодоступних джерел, і які існують види таких джерел (Мережа Інтернет, публічні урядові дані, академічні публікації, «сіра» література); було розкрито тему тенденції використання OSINT-технологій у різних сферах сьогодення.

Також було проведено детальний огляд переваг і недоліків OSINT розвідки, у тому числі при застосуванні приватними організаціями. Детально розкрито кожен етап OSINT розслідування і його особливості.

Було проведено огляд дисциплін розвідданих, включно із HUMINT, SIGINT, GEOINT, MASINT. Розкрито тему впливу розвідки з відкритих джерел на стан міжнародної безпеки й на те, як формувалася тенденція застосування різних дисциплін розвідки у світі.

РОЗДІЛ 2. АНАЛІЗ ІНСТРУМЕНТІВ OSINT Й ІДЕНТИФІКАЦІЯ ЗАГРОЗ БЕЗПЕКИ БІЗНЕСУ

2.1 Аналіз основних тактик збору даних

Досліджуючи мережу, людина стикається з чималими обсягами загальнодоступної інформації, яка доступна для перегляду й аналізу. Часто достатньо просто ввести потрібне словосполучення в Інтернеті, аби відшукати тисячі варіантів ресурсів за обраною тематикою.

Однак специфікації деяких платформ впроваджують такі обмеження, при яких отримати розвідувальну інформацію може бути дещо складніше. Більшість популярних сучасних платформ і веб-сайтів вимагають реєстрації для входу. це створює нове, більш захищене середовище, у якому аналітики не мають змоги виконувати лише пасивний збір інформації. Для доступу до необхідної інформації користувачі повинні створювати облікові записи на таких платформах і усувати межі для входу. Тому за таких умов з’являється необхідність у коригуванні методів й підходів збору даних на веб-просторах із сильнішим захистом. Саме в цьому полягає головна різниця між активною і пасивною формами OSINT.

Розвідка на основі відкритих джерел передбачає три різні тактики збору в залежності від контакту з об’єктом дослідження: пасивний, напівпасивний і активний.

Пасивний збір інформації є одним із найбільш розповсюджених тактик збору даних, так як він передбачає отримання інформації, що генерує досліджуваний об’єкт, через «тихе» спостереження за ним. Така форма збору є влучно застосовувана за наявності задачі не бути викритим досліджуваним об’єктом під час діяльності розвідки. З іншого боку, при такій формі діяльності може виникнути складність із її технічною реалізацією, тому що при цьому не буде надсилатися трафік із хостів чи сервісів до досліджуваної організації. За такого підходу збору буде підлягати виключно архівна інформація, або збережені дані, які у свою чергу

матимуть ризик бути неактуальними, неправильними; обмеженість у результатах також може мати місце.

Найчастіше OSINT виконується саме використовуючи пасивний метод збору інформації, так як проводиться із застосуванням загальнодоступних ресурсів, віддалено. Як недолік пасивного збору даних можна виділити складність здійснення глибокого пошуку й аналізу достовірних даних. При цьому може використовуватися браузер для анонімності TOR, технології VPN, віртуальні машини [15] [16].

Напівпасивний метод збору даних OSINT - більш технічний за своєю природою, знаходиться між активним і пасивним процесом збору даних. Цей метод збору даних відправляє невеликий обсяг трафіку на цільові сервери з метою отримання загальної інформації про них. Щоб не привертати уваги до розвідувальних операцій, цей трафік намагаються зробити схожим на звичайний інтернет-трафік. Таким чином, не здійснюється поглиблене дослідження інтернет-ресурсів об'єкта, а лише проводиться «легке» розслідування, не викликаючи жодної тривоги (попереджень) в групі, яка є ціллю досліджень [25]. Атаки грубої сили або поглиблені запити в цьому випадку не застосовувані.

Активна тактика збору розвідувальної інформації дозволяє безпосередньо взаємодіяти із системою та збирати інформацію про неї. Цей процес включає збір технічних даних про IT-інфраструктуру цілі за допомогою пошуку відкритих портів, сканування вразливостей через версії системи Windows із невстановленими патчами, сканування додатків веб-сервера тощо. Після того, як дані були виявлені, наступним кроком є передача їх на сервери зберігання для подальшого аналізу. Цей трафік буде виглядати як підозріла чи загрозлива поведінка і, швидше за все, залишить сліди в Системі виявлення вторгнень (IDS) або Системі запобігання вторгненням (IPS) цілі. Хоча інформація є загальнодоступною і просто знаходиться незахищеною на серверах і мережах цілі, вона все одно може бути сприйнята як хакерська атака [26].

Активний збір інформації включає в себе проведення атак соціальної інженерії на ціль. Активний OSINT, з іншого боку, відноситься до інформації, яка

активно шукається, часто через джерела, які потребують логіну або іншого узгодженого дозволу, який не легко отримати [15].

Збір розвідувальної інформації у загальнодоступному просторі відрізняється за складністю; дослідник повинен володіти навичками застосування різних наборів технологій аби зібрати повний спектр інформації. При цьому розуміння типів розвідданих із відкритих джерел і методів їх збору може допомогти вирішити, куди інвестувати час і ресурси при створенні індивідуального OSINT-інструментарію [27].

2.2 Аналіз інструментів OSINT та їх типів

Інструменти OSINT можна розділити на три основні категорії у залежності від того, на яку діяльність вони націлені:

- Інструменти виявлення: інструменти, які дозволяють шукати дані, які вже перебувають у мережі. Найкращим прикладом є пошукова система Google. Хоча може здатися, що це проста пошукова система, але насправді Google індексує і сканує безліч веб-сайтів, що, у свою чергу, дає величезний потенціал для виявлення нової інформації. Хорошим прикладом постає інструмент Shodan, який нижче буде описано.
- Інструменти вилучення: після виявлення дані необхідно вилучити і зібрати в безпечному місці. Ці інструменти гарантують, що тільки необхідні дані будуть відфільтровані для вилучення, щоб уникнути об'ємних передач (які можуть «насторожити» ціль), а також уникнути непотрібних даних, які можуть зіпсувати інформацію.
- Інструменти агрегації: після того, як були зібрані всі релевантні дані, є потреба у їх подальшому співвіднесенні та компіляції у функціональний, легко засвоюваний формат.

Звичайно, існують інструменти, які мають всі вищеперераховані функціональні можливості, включені в один пакет; здебільшого такі інструменти

потребують передплати для того, щоб отримати доступ до повного їх функціоналу, або є повністю платними рішеннями.

Перелік інструментів для пасивної розвідки варто почати з Google Dorks. Google Dorking надає можливість розгортати більш широкий пошуковий процес. Пошукові системи зазвичай індексують хедери й наповнення веб-сторінок, а для оптимізації пошукових запитів зв'язують їх. Google Dorking (або ж Google Hacking) дозволяє дещо модифікувавши звичний пошуковий термін у стрічці пошуку, додавши спеціальні оператори пошуку, відшукати такі фрагменти тексту загальнодоступних веб-сторінок, які будуть свідчити, до прикладу, про наявність версій уразливих веб-додатків. Також якщо пошук націлений на конкретну компанію, можна за допомогою цієї техніки відшукати звіти, податкові декларації, які можуть не прослідковуватися при стандартному пошуку й не бути на веб-сайтах цих компаній.

До того ж, пошук через Dorking не вимагає наявності чималих технічних знань від користувача; проте потрібно розуміти базовий синтаксис пошуку: символи (також називаються фільтрами, операторами) та ключові слова (наприклад, «intext:», «inurl:», «site:», «language:») [17]. Такі ключові слова вкінці містять двокрапку «:», потім пошукове слово без пробілу [18]. Простий семантичний запит базується на семантичному методі пошуку інформації чи методом вводу питання повністю, чи через відбір ключових слів. Поширені методи Google Dorking:

- Allintitle: - виявляє тільки сторінки з повним текстом пошуку в заголовку веб-сторінки.
- Intitle: - визначає будь-яку згадку пошукового тексту в заголовку веб-сторінки.
- Intext: - визначає тільки сторінки, що містять весь текст пошуку в URL-адресі веб-сторінки.
- Site: - обмежує результати пошуку вказаним типом файлу.
- Inurl: - визначає будь-яку згадку пошукового тексту в URL-адресі сторінки.

- Around (X): - пошук двох різних слів в межах X слів одне від одного.
- Cache: - показує найсвіжіший кеш вказаного сайту.
- Filetype: - обмежує результати пошуку тільки вказаним типом файлу [24].

Проте техніка Dorking застосовувана не лише у пошуковику Google: її можна впроваджувати й у інших популярних середовищах, наприклад, у DuckDuckGo, Bing, Yahoo. Можна виявляти різні типи «забутих» файлів, що є все ще доступні на просторах Інтернету [19].

Ще одним інструментом для пасивного OSINT є сервіс Shodan. Shodan не шукає веб-сайти, як, наприклад, Google, а підключені по IPv4-пдресах до Інтернету пристрої (камери відеоспостереження, роутери, датчики безпеки). Він виступає як пошукова система, яка сканує усі загальнодоступні системи з допомогою фільтрів, аби відшукати конкретні пристрої із зазначеними відкритими портами, операційними системами. Shodan індексує банери, на яких є відкриті певні порти. Прикладом відкритих для Інтернету систем є веб-камери, сервери, маршрутизатори. За допомогою Shodan можна сканувати порти знайдених систем, ідентифікувати сервіси, які на відкритих портах працюють і визначити версії таких сервісів. Shodan має функцію генерації коротких звітів щодо, наприклад, деталей CVE-коду вразливостей. Робота ресурсу ґрунтується на запитах з'єднання з безліччю можливих IP-адрес, та індексуванні отриманої шляхом цих запитів з'єднань.

Пошук у Shodan може здійснюватися на основі назви пристрою, IP-адреси, міста чи інших технічних характеристик. Для детектування пристроїв, що належать певній компанії, слід використовувати параметр org:, після нього вказавши назву організації, наприклад: org:Samsung. Параметр port: дозволяє виявити відкриті порти систем. Параметр os: використовується для того, щоб задати фільтр цілей відповідно до їх ОС. Тобто можна, наприклад, виявити певні пристрої зі встановленими ОС, які мають уразливості, із подальшим сценарієм щодо експлуатації цих уразливостей в компрометації цих систем. У відкритому доступі можна знайти спеціальні заготовки з інструкціями щодо використання Shodan [20].

Maltego є програмою для збору розвідданих із відкритим кодом, є частиною дистрибутиву Kali Linux, яка надає можливість збирати інформацію про конкретну ціль. Maltego виконує низку перетворень, так звані «трансформації», які дозволяють автоматично виконувати техніки пасивної розвідки. Такі перетворення включають пошуки DNS-записів із різних джерел, повертають адреси електронної пошти, номери телефонів, IP-адреси, номери AS та інші види інформації. До того ж, Maltego надає інтуїтивно зрозумілий і зручний інтерфейс для перегляду інформації з можливістю подальшої ідентифікації слабких місць мішені [21][22].

Ще одним ефективним інструментом для пасивного OSINT є «Have I been Pwned?». Цей сервіс дозволяє перевірити наявність скомпрометованих облікових даних поштових скриньок. Він архівує й використовує численні відомі витоки баз даних і перевіряє, чи введена електронна адреса була виявлена серед цих витоків. Такі витоки зазвичай відбуваються з різних джерел, і багато з них містять численні набори даних різних типів: адреси електронної пошти, паролі, імена, імена користувачів, хеші паролів, інформація платіжних карток, номери телефонів, адреси та інше. Серед джерел, із яких трапилися одні з найбільших витоків даних (архівовані «Have I been Pwned?»), є Collection #1 (772904991 записів), Verifications.io (763117241 записів), Onliner Spambot (711477622 записів); при цьому витоки даних ставалися і з таких популярних платформ, як Facebook, LinkedIn, Adobe, VK, Dropbox та інші [21][23].

Перевірити можна як власну електронну адресу, так і зібрані іншими методами (сервісами) електронні адреси: наприклад, на основі зібраних даних згадуваним вище інструментом пасивної розвідки Maltego.

Доволі потужним OSINT-інструментом як пасивної, так і активної розвідки також є Spiderfoot. Він є частково безкоштовним інструментом OSINT-розвідки, який інтегрується з різними джерелами даних і автоматизує збір даних. Spiderfoot ґрунтується на зборі й аналізі даних про IP-адреси, імена користувачів, домени, номери телефонів, CIDR діапазони та інші конфіденційні дані. Інструмент надає зрозумілий на інтуїтивному рівні графічний веб-інтерфейс і містить як інтерфейс командного рядка (CLI), так і вбудований веб-інтерфейс. Модулі SpiderFoot

запрограмовані на взаємодію один з одним, що дозволяє всім пов'язаним модулям використовувати одні й ті ж дані про ціль. При виборі налаштування «пасивне сканування», Spiderfoot не відправлятиме жодних прямих запитів із комп'ютера, видаливши модулі, які намагаються встановити прямі з'єднання.

SpiderFoot HX є безкоштовною онлайн-версією інструменту Spiderfoot, і надає можливість провести п'ять сканувань на місяць. Після вибору цілі (або групи цілей у вигляді доменних імен, IP-адрес, імен користувачів тощо) інструмент запускає основне сканування, яке автоматично починає шукати інформацію із більш ніж ста відкритих джерел інформації.

Недоліком інструменту Spiderfoot є те, що сторінки, позначені як "noindex", не відображатимуться - вони дають неповне уявлення про справжній масштаб поверхні атаки [28].

Recon-ng є абсолютно безкоштовним CLI-інструментом із відкритим вихідним кодом, є створеним для веб-розвідки. Інструмент має модулі за замовчуванням, які також мають відкритий вихідний код; також існує комерційна платформа для додавання ще більшої кількості функцій. Оскільки це інструмент з відкритим вихідним кодом, він продовжує розвиватися і рости, а спільнота розробників продовжує робити свій внесок у нього. Написаний на мові Python, Recon-ng призначений виключно для веб-розвідки з відкритим вихідним кодом. Тому він не може бути використаний для експлойтів. Після того, як інформація зібрана, вона зберігається в базі даних, яка потім може бути використана для створення глибоких користувацьких звітів. Потім потрібно експортувати дані з бази даних та імпортувати їх у інший інструмент візуалізації даних для подальшого їх аналізу. Висока деталізація, яку надає Recon-ng, вимагає часу для повного вивчення та використання всіх функцій інструменту.

Metasploit є активним OSINT-інструментом для отримання чималої кількості необхідної інформації про ціль - комп'ютер, мережа - і подальшого використання будь-якої вразливості, яка може бути ідентифікована; це сканер вразливостей і інструмент для тестування на проникнення. Ефективність такої системи полягає у тому, що Metasploit надає інструменти для дослідження системи та виявлення

інформації про компоненти безпеки й можливі шляхи проникнення в мережу, а після чого вона автоматично копіює й використовує ці дані як інструменти атаки для реалізації компрометації системи. Metasploit має сім модулів, які можна використовувати для різних кампаній зі збору розвідувальної інформації. Ці модулі вирішують конкретні проблеми, такі як, наприклад, подолання захисту (шифратори), запуск скриптів і коду шляхом використання переповнення буфера (NOP) або виконання завдань після компрометації системи (post). Як тільки доступ до системи буде отриманий, він може практично «захопити» кожен пристрій у ній. Metasploit може націлюватися на пристрої, що працюють практично під будь-якою операційною системою: Windows, Android, Linux, macOS та багато інших.

Metasploit можна запустити з Windows, Linux і macOS. Він є одним із найбільш популярних інструментів для хакерів і орієнтований на більш технічно обізнаних користувачів.

Aircrack-ng є інструментом для тестування на проникнення у бездротову мережу, який має чотири основні функції:

1. Моніторинг пакетів - перехоплення кадрів і збір WEP IV (векторів ініціалізації); якщо додано GPS, він може реєструвати положення AP (точок доступу).
2. Тестування на проникнення - шляхом виконання атак на впровадження пакетів, фальшивих точок доступу, атак повторного відтворення тощо, для перевірки безпеки мережі.
3. Аналіз продуктивності - тестування можливостей WiFi та драйверів, тест на наявність слабких місць, які допомагають контролювати безпеку.
4. Тестування захищеності паролів - злам паролів на WEP та WPA PSK (WPA 1 та 2).

Хоча інструмент був розроблений в першу чергу для Linux, існують версії для Windows, OS X і FreeBSD. Aircrack-ng є CLI-інструмент, тобто він може бути легко налаштований для задоволення унікальних вимог за допомогою спеціальних скриптів.

Потужність Aircrack-ng значно зменшується за впровадження ефективного шифруванням передачі даних. Тестувальники на проникнення і менеджери системної безпеки можуть використовувати цей інструмент для підтвердження того, що безпека передачі є достатньою [29] [30].

OSINT-інструмент активної OSINT-розвідки Nmap, або «Network Mapper» був створений досить давно і все ще використовується для спостереження за мережевою безпекою; його можна використовувати для виявлення або тестування з метою перегляду статусів хостів і збору інформації, такої як спільні дані, операційні системи тощо, для виявлення вразливостей. Nmap застосовується головним чином для мапування мереж і допомоги розпізнавати пристрої, підключені до серверів. Він відстежує відкриті порти і виявляє ризики безпеки без залучення зовнішніх команд або процесів конфігурації. Ключовими особливостями Nmap можна вважати наступні:

- Інструмент надає можливість проведення мережевого мапування та аудиту безпеки.
- Має кращу підтримку IPv6.
- Підтримується багатьма операційними системами, такими як Linux, Microsoft Windows, IRIX, Mac OS тощо.

З часом Nmap став більш потужним і тепер надає графічний інтерфейс (Zenmap) [31].

Одним із найпростіших інструментів для збору та доступу до публічної інформації за межами мережевого периметру організації є theHarvester. Він шукає цінну інформацію про адреси електронної пошти, віртуальні хости, імена субдоменів, та відкриті порти будь-якої організації. Цей інструмент дуже корисний при визначенні обсягу завдання тестування на проникнення і допомагає в якості розвідувального кроку перед ним. theHarvester задіює для OSINT-збору різноманітні соціальні мережі й поширені пошуковики - Google, Bing, Duck Duck Go. theHarvester дозволяє експортувати XML-звіти та здійснювати пошук доменів по всіх підтримуваних джерелах.

theHarvester допомагає тестерам на проникнення розпізнавати сліди клієнтів у мережі Інтернет, допомагає забезпечити безпеку організації шляхом визначення зовнішніх загроз [32]

2.3 Ідентифікація загроз безпеки бізнесу з допомогою інструментів OSINT

2.3.1 Нормативно-правове регулювання

Чинна нормативно-правова база OSINT базується на Директиві Директора Національної Розвідки (2006) ICD 301 "Національний план з Розвідки на основі відкритих джерел".

Правоохоронне OSINT-співтовариство застосовує розвіддані з відкритих джерел для прогнозування, запобігання, розслідування і судового переслідування злочинів, включаючи тероризм. Пошук через соціальні мережі та DarkNet відіграє значну роль в їх роботі, так само як і аналіз з'єднань. Зважаючи на величезний обсяг контент-трафіку, що проходить через Інтернет через платформи соціальних мереж, правоохоронні органи не повинні ігнорувати акаунти в соціальних мережах як ресурс для виявлення доказів, що потенційно можуть мати відношення до цілого ряду кримінальних розслідувань.

Ще одна група важливих цілей досягається за допомогою OSINT: оцінка ризиків, коли інформація збирається для прийняття рішення. Процедура «due diligence» може проводитися як банком, так і консалтинговою компанією, коли основною метою є проведення комплексної оцінки вартості активу. У таких випадках має значення репутація, зв'язки та фінансовий стан бенефіціарів. Такі перевірки, як і пошук афілійованості між працівниками та контрагентами, проводяться і в бізнесі. Питання в тому, наскільки швидко, ефективно і точно це може бути проведено. Інтернет, особливо соціальні мережі, дає нам величезний обсяг даних для аналізу, але збирати їх вручну було б занадто складно, довго й неефективно.

Малий бізнес також, мабуть, найбільше втрачає від руйнівної кібератаки. Сьогодні що компанії з менш ніж 500 працівниками втрачають в середньому 2,5

мільйона доларів за одну атаку. Втрата такої суми грошей в результаті кібератаки є руйнівною для малого бізнесу, до того ж існують великі репутаційні збитки, які виникають внаслідок кібератаки.

Приватні корпоративні служби безпеки також охоче застосовують OSINT-інструменти. Вони проводять індивідуальні перевірки: власних співробітників, топ-менеджменту, працівників, керівників та акціонерів своїх контрагентів. Тут спрацьовує режим "Знай свого клієнта" (англ. KYC). Питання перевірки, чи компанія офшорна, хто є її реальним власником, чи не була вона задіяна у нелегальному бізнесі, є вкрай важливо знати перед укладенням будь-якої великої угоди.

Перевірити на афілійованість фізичних або юридичних осіб - ось основна мета, яка зазвичай обрисовується. Служби економічної безпеки проводять моніторинг внутрішніх угод на предмет наявності прихованих інтересів. Наприклад, якщо менеджер із закупівель укладає угоди з компаніями, що належать членам його сім'ї. Перед кожним злиттям чи поглинанням відділ транзакційних послуг проводить перевірку: чи не перебуває фірма, що купується, під контролем криміналітету. Таким чином, великі компанії прагнуть мінімізувати репутаційні ризики як для компанії, так і для акціонерів. Кожна серйозна фірма зазвичай має власний список надійних і небажаних контрагентів. У будь-якому випадку, керівництво завжди має знати, хто стоїть за тим чи іншим суб'єктом.

Випадки застосування OSINT у страховому бізнесі стосуються як аналізу персональних даних компанії, так і бізнес-аналітики. Величезна федеральна компанія має змогу прослідкувати, що в одному окремому регіоні значно зросли платежі за одним окремим страховим продуктом.

HR-відділи використовують OSINT для перевірки чинних або потенційних працівників своїх компаній, наприклад, чи не публікують вони негативні дані про компанію у своїх соціальних мережах, чи не розголошують конфіденційну інформацію. Іноді це відбувається не зі злого умислу, а випадково. Наприклад, спланована перевірка афілійованості через соціальні мережі працівників регіональної філії компанії може показати, що один з менеджерів страхував своїх

друзів та родичів з метою подальшої реєстрації страхових випадків та виплат. Така обізнаність ще не є доказом вини особи, але, безумовно, є предметом внутрішнього розслідування.

Деякі громадські організації здійснюють постійний моніторинг загроз, в тому числі терористичних. Наприклад, одна з єврейських дослідницьких організацій зі США використовує інструменти OSINT для пошуку саме з цією метою. Вони хочуть уникнути нападів або інцидентів під час своїх заходів, тому проводять такий моніторинг з метою їх попередження.

2.3.2 Основні загрози бізнесу

Беручи до уваги всі наведені раніше факти, можна з упевненістю стверджувати, що бізнес повинен знати про загрози та способи їх запобігання. Компанії можуть стикатися із п’ятьома основними ризиками:

1) Фішингові атаки, компрометація ділової електронної пошти (BEC)

Найбільшою, найшкідливішою та найпоширенішою загрозою, з якою стикається малий бізнес, є фішингові атаки. На фішинг припадає 90% всіх порушень, із якими стикаються організації, їх кількість зросла на 65% за останній рік, і вони завдають чималих збитків для бізнесів по всьому світу щороку. Фішингові атаки відбуваються, коли зловмисник видає себе за довірену особу і спонукає користувача перейти за шкідливим посиланням, завантажити шкідливий файл або надати йому доступ до конфіденційної інформації, даних облікового запису або облікових даних.

Шахрайство з компрометацією ділової електронної пошти (BEC) передбачає заманювання в пастку керівників великих організацій, включаючи осіб, які приймають рішення на найвищому рівні, які були обмануті за допомогою атак соціальної інженерії, щоб перевести кошти на шахрайські рахунки.

2) Шкідливе ПЗ

Шкідливе програмне забезпечення є другою великою загрозою, з якою стикається малий бізнес. Воно охоплює різні кіберзагрози, такі як трояни та віруси. Це різноманітний термін для позначення шкідливого коду, який зловмисники

створюють для отримання доступу до мереж, крадіжки даних або знищення даних на комп'ютерах. Шкідливе програмне забезпечення зазвичай походить від завантаження шкідливих веб-сайтів, спаму в електронній пошті або від підключення до інших заражених комп'ютерів або пристроїв.

3) Програми-вимагачі

Програми-вимагачі є однією з найпоширеніших кібератак, що вражають тисячі підприємств щороку. Останнім часом вони стали більш поширеними, оскільки є однією з найбільш прибуткових форм атак. Зловмисники часто розробляють шкідливе програмне забезпечення так, щоб воно поширювалося по всій інфраструктурі організації, націлюючись на всю базу даних і файлові сервери, щоб більш ефективно змусити компанію заплатити викуп. Програми-вимагачі шифрують дані компанії, щоб унеможливити їх використання або доступ до них, а потім змушують компанію заплатити викуп за розшифрування й розблокування даних. Це ставить компанії перед складним вибором - заплатити викуп і потенційно втратити величезні суми грошей, або ж завдати шкоди своїм сервісам через втрату даних.

У міру того, як атаки стають все більш серйозними, зловмисники також застосовують тактику додаткового зовнішнього тиску, наприклад, погрожуючи розголосом конфіденційної інформації, відстороненням керівників або інформуванням клієнтів про те, що компанія не готова платити за захист їхніх даних, аби підвищити ймовірність сплати викупу.

4) Слабкі паролі

Ще однією великою загрозою, з якою стикається малий бізнес, є використання співробітниками слабких або легко вгадуваних паролів. Багато малих підприємств використовують декілька хмарних сервісів, які вимагають різних облікових записів. Ці сервіси часто можуть містити конфіденційні дані та фінансову інформацію. Використання паролів, які легко вгадуються або є занадто простими, або використання одних і тих же паролів для декількох облікових записів може призвести до компрометації цих даних.

Безпека паролів повинна бути більш пріоритетною, починаючи з рівня керівництва підприємств і закінчуючи окремими особами, які працюють вдома. Вкрай важливо, щоб підприємства вживали заходів, блокуючи слабкі та скомпрометовані паролі, забезпечуючи дотримання вимог щодо довжини паролів, впроваджуючи верифікацію користувачів у службі підтримки та проводячи аудит середовища підприємства з метою виявлення вразливостей, пов'язаних з паролями.

5) Внутрішні загрози

Останньою основною загрозою, з якою стикається малий бізнес, є внутрішня загроза. Внутрішня загроза - це ризик для організації, спричинений діями працівників, колишніх працівників, ділових підрядників або партнерів. Ці суб'єкти можуть отримати доступ до критично важливих даних про компанію, і вони можуть спричинити негативні наслідки через, наприклад, жадібність, або просто через незнання та необережність. Це зростаюча проблема, яка може поставити під загрозу співробітників і клієнтів або завдати компанії фінансових збитків. У малому бізнесі інсайдерські (внутрішні) загрози зростають, оскільки все більше співробітників мають доступ до декількох облікових записів, які містять більше даних. Дослідження показують, що 62% усіх працівників повідомили, що мають доступ до облікових записів, які їм, найімовірніше, не потрібні [33].

6) Порушення даних

Порушення даних відбувається щоразу, коли конфіденційні дані ненавмисно розкриваються, або коли несанкціонований суб'єкт здійснює їх витік чи крадіжку. Порушення може статися випадково, через недбалість або в результаті цілеспрямованої атаки. Інцидент порушення може варіюватися від одного до понад 1 мільйона записів порушених даних. Однак за останні кілька років події порушення почали викривати мільярди записів, що містять конфіденційні дані та інформацію про клієнтів. Часто порушення, які призвели до витоку найбільшої кількості даних, є результатом людських помилок, що виникають через поганий контроль безпеки та невиправлені системні вразливості.

7) Підміна SIM-карти

Термін "підміна SIM-картки" історично відноситься до заволодіння телефонними номерами за допомогою різних методів. Вони включали повторне використання паролів, атаки соціальної інженерії від шахраїв, що видавали себе за фахівців з обслуговування клієнтів, а також використання витоку баз даних та особистої інформації (наприклад, номерів соціального страхування (SSN) для полегшення захоплення телефонних ліній) [34].

2.3.3 Особливості застосування OSINT для безпеки бізнесу

Методи OSINT мають вирішальне значення для надання знань аналітикам розвідки загроз, приватним детективам або будь-яким старшим консультантам з питань безпеки, щоб досягти успіху в своїй галузі. За допомогою розвідки на основі відкритих джерел можна отримати сотні тисяч результатів, здебільшого, коли задіяні зовнішні та внутрішні ресурси. Набагато дешевшим є підхід, коли збір розвідданих відбувається заздалегідь, і краще, коли проблеми вирішуються на випередження, ніж є викритими в режимі реального часу, реагуючи на несподіваний інцидент. Важливо не нехтувати застосовуванням технологій OSINT, аби не допускати інцидентів, або принаймні пом’якшити їх вплив на стан захищеності організації.

Розвідка відкритих джерел інформації при її інтегруванні у систему безпеки компанії здатна забезпечити наступні аспекти захищеності:

- Виявлення витоків даних. Випадкові витоки даних співробітниками та іншими зацікавленими сторонами становлять недооцінену загрозу для організацій. Наприклад, працівник може опублікувати фотографію свого робочого бейджа в соціальних мережах. Зловмисники можуть використати таку інформацію для створення фальшивих облікових даних та отримати несанкціонований доступ до об'єктів компанії. Але за допомогою моніторингу відкритих каналів аналітики можуть виявити і усунути ці порушення до того, як виникнуть проблеми.
- Кібербезпека. Розвідка дозволяє технічним командам виявляти і виправляти вразливості в мережевих системах. Це може дати організаціям можливість швидше реагувати на порушення, які вже сталися. Або вони можуть

бути в змозі зупинити кібератаки ще до того, як вони відбудуться – превентивні міри.

- Аналіз ризиків. OSINT може перехоплювати розмови, надаючи уявлення про спосіб мислення і думки місцевих жителів у регіоні. Це може бути безцінною інформацією для осіб, які приймають рішення при розгляді нового проекту або розширенні діяльності на іншій території.

- Захист бренду. Несанкціонована діяльність під логотипом організації може зашкодити репутації фірми (наприклад, видача себе за керівника, створення веб-сайтів з використанням друкарських помилок або шахрайство при працевлаштуванні). Це також може включати в себе злочинну діяльність щодо власності компанії, наприклад, торгівлю людьми. Однак розвіддані з відкритих джерел дозволяють організаціям виявляти і вирішувати ці проблеми.

- Реагування на кризові ситуації. Люди часто повідомляють про події в соціальних мережах за кілька годин або навіть днів до того, як їх підхоплять ЗМІ. Постійно спостерігаючи за цими каналами, команди безпеки можуть бути попереджені про надзвичайну ситуацію майже одразу після її виникнення. Крім того, коментарі, зібрані через відкриті джерела, такі як фотографії, аудіо та коментарі, можуть дозволити аналітикам більш ефективно реагувати.

- Захист працівників і керівників корпорації. OSINT є важливим інструментом для охоронців при охороні високопоставлених осіб. Наприклад, перебуваючи в дорозі, співробітники служби безпеки можуть сканувати відкриті джерела для проведення регіональної оцінки ризиків, виявлення можливих ризиків і розробки альтернативних планів подорожі. Крім того, високопоставлені особи часто стають об'єктами насильницьких погроз в Інтернеті. Інструменти OSINT дозволяють службам безпеки виявляти загрозливі повідомлення, підтверджувати загрозу та планувати відповідні заходи реагування.

- Захист інтелектуальної власності. Сучасне програмне забезпечення OSINT може виявити злочинні мережі в Інтернеті, які займаються підробкою, піратством контенту і нелегальним потоковим мовленням. Команди безпеки також використовують методи розвідки з відкритих джерел для виявлення зловмисних

інсайдерів, які продають в Інтернеті закриті секрети компанії, такі як патенти, плани досліджень або дорожні карти продуктів.

- Боротьба зі шахрайством та запобігання втратам. Групи по боротьбі з шахрайством і запобіганню втрат потребують актуальної інформації про новітні методи крадіжок. Злочинці часто хизуються своїми «досягненнями» в Інтернеті. Ця інформація дозволяє організаціям краще захистити свої операції від крадіжок і шахрайства.
- Захист ланцюгів поставок. Збої в ланцюгах поставок можуть призвести до зриву термінів поставок продукції. Уникнення таких проблем вимагає наявності всієї доступної інформації про нові та існуючі загрози. Звичайно, нові технології, такі як датчики Інтернету речей та блокчейн, відіграють певну роль у цьому процесі. Але OSINT надає особам, які приймають рішення, контекст, необхідний для ефективної адаптації в умовах кризи [12].

2.4 Висновки до другого розділу

У ході написання другого розділу було проаналізовано основні тактики збору даних (активний, напівпасивний, пасивний збір інформації) та описані задачі, які вони можуть вирішувати.

Також була досліджена класифікація інструментів OSINT (інструменти виявлення, вилучення й агрегації). Були розглянуті OSINT-інструменти збору даних (Maltego, SpiderFoot, Shodan, Recon-ng та інші), та були описані принципи їх роботи.

Також було детально описано нормативно-правове регулювання OSINT, було ідентифіковано основні загрози безпеки бізнесу і охарактеризовані особливості застосування OSINT для безпеки бізнесу.

Окрім цього, було сформульовано вимоги щодо проведення OSINT для бізнесу, які полягають у дотриманні нормативно-правового регулювання процесу OSINT, етичних норм; також це передбачає дотримання меж розвідки, тобто не заходити за границі, визначені замовником.

РОЗДІЛ 3. ПРАКТИЧНЕ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ OSINT ДЛЯ ВИЯВЛЕННЯ ЗАГРОЗ БЕЗПЕКИ БІЗНЕСУ

3.1 Збір інформації про цільову особу компанії

Припустимо, за допомогою технології OSINT нам потрібно зібрати якнайбільше інформації про ціль, пов’язану із певною компанією – тобто такі дані, як:

- Ім’я і прізвище;
- адреси електронної пошти (корпоративні й особисті);
- номер телефону;
- посилання на сторінки в соціальних мережах;
- кар’єрну історію.

Для проведення людських розслідувань з особистої практики варто використовувати не глобальні інструменти сканування, а задіювати кілька різних ресурсів у залежності від завдань, які потрібно виконати.

Цільовою організацією у нашому випадку буде американська технологічна компанія Dell Technologies. Для початку ми скористалися безкоштовною версією веб-інструменту пошуку людей і компаній «snov.io», де виконали пошук за доменом «dell.com» і ідентифікували цільову компанію Dell Technologies. Результатом була інформація про цю компанію із позначенням кількості працівників, адреси, дати заснування, адреси веб-сайту, індустрії діяльності, посилання на соціальну мережу, та іншими афілійованими компаніями, деталі зображено на рисунку 3.1 [35].

Рисунок 3.1 – Деталі про компанію Dell

Окрім вищенаведених результатів, OSINT-пошук містив таку цінну інформацію, як імена й прізвища працівників, їх роль в організації з можливістю перевірити електронну адресу. У навчальних цілях ми обираємо ціль для подальшого дослідження серед списку, який включає більше 13000 записів імен й прізвищ.

«snov.io» надав такі дані про ціль, як: ім’я й прізвище, діючу робочу адресу електронної пошти й посаду в компанії, адресу й країну, місто локації, відображені на рисунку 3.2.

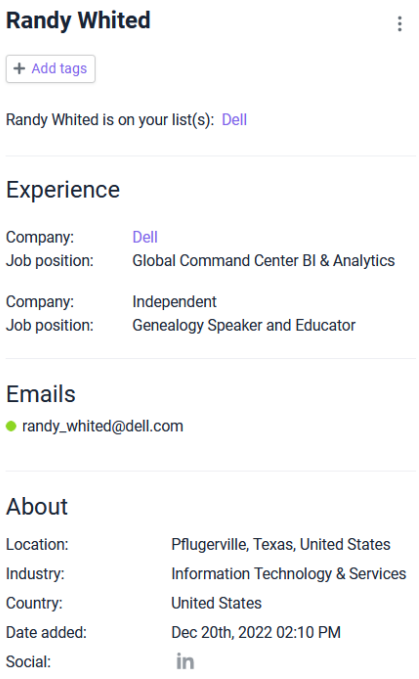

Рисунок 3.2 –Інформація про працівника компанії Dell, отримана з ресурсу «snov.io»

Також вивід містив посилання на сторінку у соціальній мережі LinkedIn. Наступним кроком буде OSINT соціальних мереж користувача Randy Whited, це дасть змогу також знайти фото цілі. Звісно, аби виконувати такий пошук, потрібно зареєструвати окремий, не пов'язаний із особою шукача, обліковий запис; налаштувати в ньому якусь соціальну активність. Бажано використовувати повністю підроблену особистість (так звані «Sock Puppets»), щоб не залишати після себе жодних слідів; ресурсом для таких маніпуляцій може стати «fakenamegenerator.com».

Під час дослідження був використаний запит, зображений на рисунку 3.3, який дав змогу шукати за іменем користувача, назвою компанії, і пошук повинен включати результати із соціальної мережі LinkedIn.

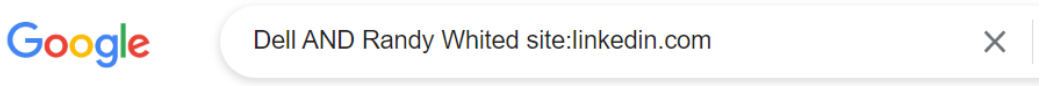

Рисунок 3.3 – Запит Google для пошуку профілю на LinkedIn

Після запиту був отриманий найбільш релевантний результат, який вів на сторінку потрібного користувача Randy Whited. Ми можемо переглянути кількість встановлених контактів користувача, місце праці – рисунок 3.4.

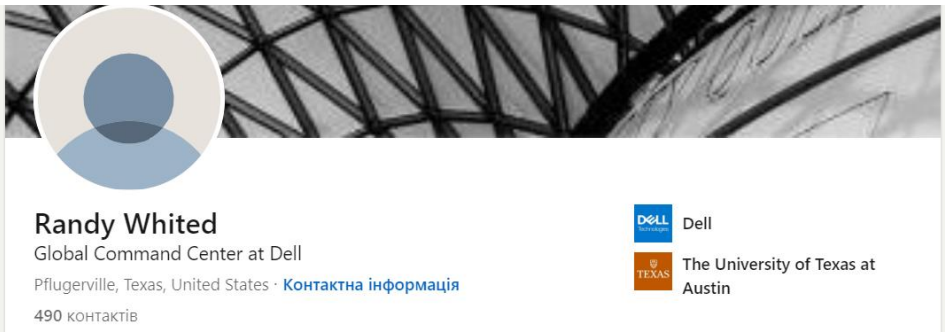

Рисунок 3.4 – Сторінка цілі у соціальній мережі LinkedIn

Окрім цього, ми можемо знайти багато інших важливих деталей щодо цього працівника, адже він активно веде сторінку в цій соціальній мережі й ділиться здобутками. На рисунку 3.5 зображена частина досвіду праці Randy Whited.

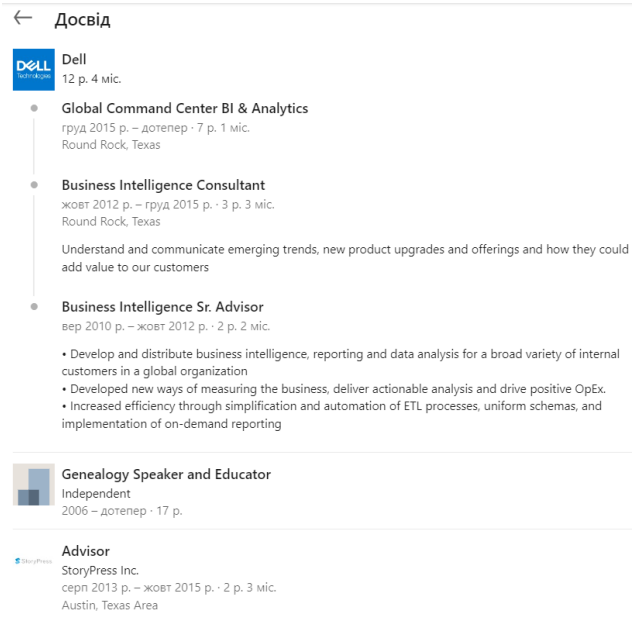

Рисунок 3.5 – Робочий досвід цілі

Також ми знаходимо інформацію щодо благочинної діяльності, пов’язаної із цільовою особою (див рис. 3.6).

Рисунок 3.6 – Інформація щодо волонтерської діяльності цілі

Аналізуючи наповнення LinkedIn-сторінки працівника Dell Randy Whited, ми отримали багато даних, окрім наведеної вище: інформація щодо ліцензій і сертифікатів, перелік навичок, рекомендації від колег-працівників, публікації, проєкти, інтереси, включно з волонтерськими; як додаток, посилання на неактивну сторінку в соціальній мережі Twitter. Це дозволяє задати вектор подальшого

дослідження – у наступному кроці буде проведений пошук особистих зображень цільової особи [36].

Так як із LinkedIn ми не отримали фото цільової особи, ми використаємо дані з цієї соціальної мережі для пошуку потрібних зображень, а згодом продовжимо пошук акаунтів соціальних мереж, вже маючи зображення. Використовуючи зачіпку, що продемонстрована на рисунку 3.6, де відображене місце волонтерської діяльності - Global Family Reunion, ми задаємо у браузері Google запит, наведений на рисунку 3.7.

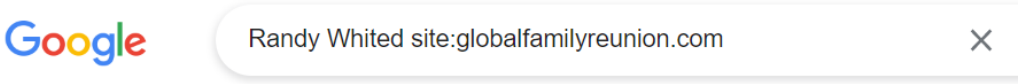

Рисунок 3.7 – Запит Google для пошуку цілі на globalfamilyreunion.com

Зображення цілі отримано серед найбільш релевантних результатів. Ми упевнені, що дане фото належить шуканій особі, адже зв'язки, вміст сайту globalfamilyreunion.com це підтверджують (див. рис. 3.8).

Рисунок 3.8 – Шукане зображення цілі

За допомогою інструменту «sherlock» запущеного на віртуальній машині Kali Linux, ми задаємо пошук за іменем користувача «randywhited» і отримуємо ряд посилань на соціальні мережі й платформи, де був знайдений обліковий запис із таким іменем користувача (див. рис. 3.9).

```
┌──(kali㉿kali)-[~/sherlock]
└─$ python3 sherlock randywhited
[*] Checking username randywhited on:

[+] About.me: https://about.me/randywhited
[+] Archive.org: https://archive.org/details/@randywhited
[+] Disqus: https://disqus.com/randywhited
[+] Duolingo: https://www.duolingo.com/profile/randywhited
[+] Enjin: https://www.enjin.com/profile/randywhited
[+] Facebook: https://www.facebook.com/randywhited
[+] Fiverr: https://www.fiverr.com/randywhited
[+] Flipboard: https://flipboard.com/@randywhited
[+] Gravatar: http://en.gravatar.com/randywhited
[+] Instagram: https://www.instagram.com/randywhited
[+] ReverbNation: https://www.reverbnation.com/randywhited
[+] Slides: https://slides.com/randywhited
[+] Smule: https://www.smule.com/randywhited
[+] Snapchat: https://www.snapchat.com/add/randywhited
[+] Strava: https://www.strava.com/athletes/randywhited
[+] Trello: https://trello.com/randywhited
[+] Twitch: https://www.twitch.tv/randywhited
[+] We Heart It: https://weheartit.com/randywhited
[+] WordPress: https://randywhited.wordpress.com/
[+] koo: https://www.kooapp.com/profile/randywhited
[+] zoomit: https://www.zoomit.ir/user/randywhited
[+] Youtube Channel: https://www.youtube.com/c/randywhited
[+] Youtube User: https://www.youtube.com/user/randywhited

[*] Results: 23

[!] End:  The processing has been finished.
```

Рисунок 3.9 – Посилання на соціальні мережі цільової особи

Вивід «sherlock» надав частину релевантних посилань на соціальні платформи randywhited, які є або були в минулому активні. Із релевантних результатів можна виділити посилання на YouTube-канал, де ми отримуємо доступ до списків відтворення користувача – рисунок 3.10 [37].

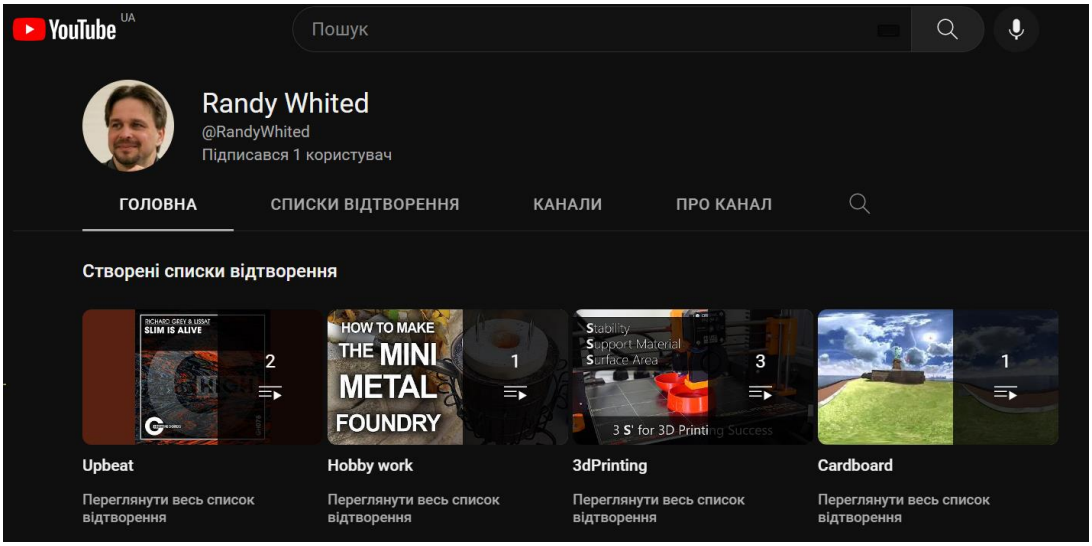

Рисунок 3.10 – Знайдений YouTube-канал randywhited

Проведений пошук у соціальній мережі Facebook за фільтрами імені, прізвища й міста проживання надав нам результат із дійсною, активною сторінкою

цільової особи, де ми отримали доступ до фото користувача, дописів, відміток – рис. 3.11 [38].

Рисунок 3.11 – Знайдений активний Facebook-акаунт цілі

Пошук у Facebook показав, що ціль має друге ім’я, і за допомогою цієї інформації й подальшого пошуку у соціальних мережах ми виявили приватну сторінку цілі в Instagram – рисунок 3.12 [39].

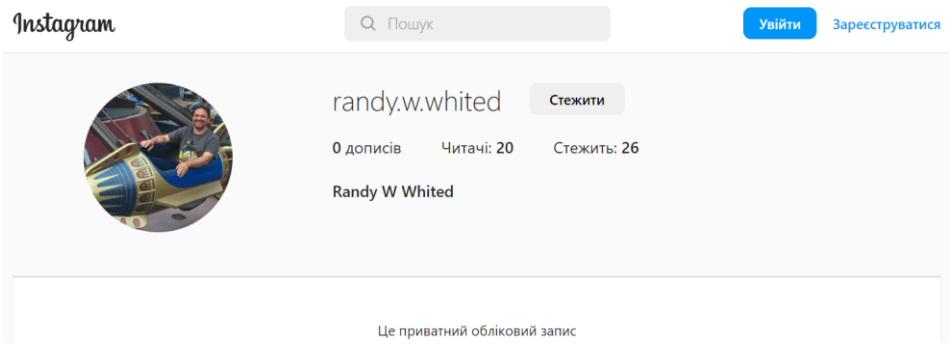

Рисунок 3.12 – Знайдена приватна сторінка Instagram цілі

Останнім кроком буде використання OSINT-ресурсу «Spokeo». Як видно на рисунку 3.13, маючи такі дані, як ім’я, друге ім’я й прізвище, місце проживання ми створили унікальний запит і отримали чимало інформації про шукану особу (знайдені дані на рисунку не відображаються повністю з етичних міркувань) [40].

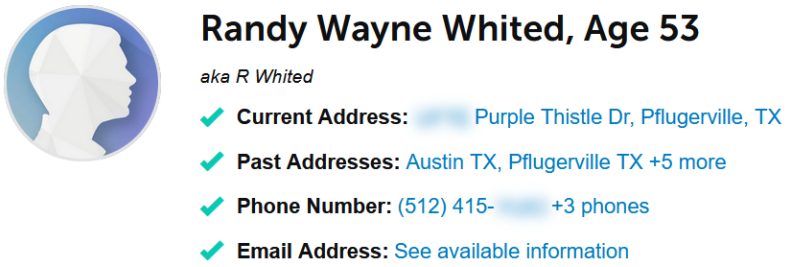

Рисунок 3.13 – Вивід «Spokeo»

У наступному дослідженні буде проведена перевірка цього ж користувача у витоках і порушеннях даних.

3.2 Ідентифікація витоків даних цільової особи компанії

Порушення даних - це дані, які стають загальнодоступними завдяки фізичним або юридичним особам, які здійснюють витік даних. Хоча сам акт порушення є незаконним, отримання та використання даних після їх витоку є законним і дуже корисним для розслідування OSINT-інцидентів.

Більшість витоків даних компаній - це просто імена користувачів/адреси електронної пошти та паролі, які, ймовірно, були отримані від нескладних хакерських команд, що сканують Інтернет у пошуках незахищених серверів, залишених відкритими для зовнішніх з'єднань. Інші витоки даних можуть включати інформацію, що дозволяє ідентифікувати особу (PII), таку як справжнє ім'я, номер телефону, адреса електронної пошти, кредитна картка, національні документи, що посвідчують особу (водійське посвідчення, паспорт, посвідчення особи), та іншу захищену інформацію. Зламані набори даних регулярно завантажуються і надаються (безкоштовно або платно) громадськості на різних сайтах для зберігання файлів, а також більш обмеженій аудиторії через форуми або ринки у DarkNet.

Дані про порушення можуть бути важливими для OSINT-розслідування, для виявлення нових зачіпок і підтвердження існуючих даних про ціль, а також для інших послуг, включаючи кредитний моніторинг і забезпечення дотримання вимог

щодо захисту даних клієнтів. З міркувань конфіденційності також важливо розуміти масштаби витоку персональних даних. При оцінці цінності витоку даних критично важливо думати не лише про кількість записів, але й про унікальність даних (якість) рівною мірою. Також варто визначити, чи дублюються дані - великі компіляції порушень однієї і тієї ж компанії, чи вони містять більш вибіркову та конфіденційну інформацію, наприклад, державні документи або приватні медичні історії.

Припустимо, є потреба в ідентифікації порушень (чи витоків) даних, пов'язаних із певною організацією. Спочатку потрібно мати набір ідентифікаторів, які, до прикладу, надає клієнт, а серед них можуть бути доменні імена. Тож за допомогою пошуку за доменним іменем із використанням певних OSINT-інструментів можна виявити електронні адреси, пов'язані з діяльністю цільової компанії, і перевірити їх на приналежність до якогось із відомих витоків даних, після чого виявити ці дані. Більшою мірою найбільш потрібними чи «небезпечними» розвідданими є саме паролі.

Для пошуку адрес електронної пошти буде використаний ресурс «Phonebook.cz», який надає можливість пошуку електронних адрес, субдоменів, URL-адрес. Для дослідження адрес електронної пошти буде використаний домен «dell.com». На рисунку 3.14 зображені результати пошуку за доменом dell.com [41].

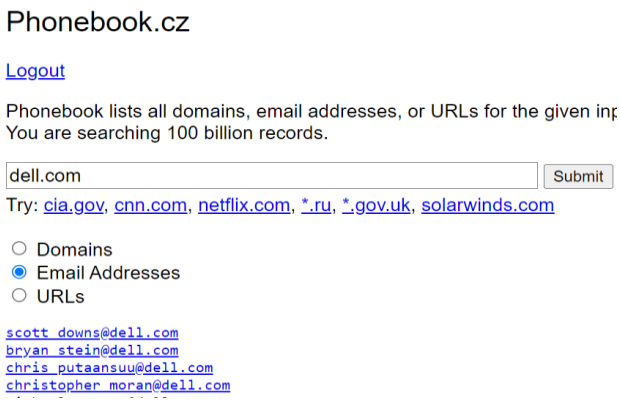

Рисунок 3.14 – Результати пошуку за доменом dell.com

Варто зазначити, що схожим за своїм функціоналом ресурсом є також «Hunter.io», проте він не надає безкоштовних результатів. Платна версія

інструменту дозволяє зробити пошук, включно й за доменним іменем, визначити найбільш поширений патерн, за яким формуються емейл-адреси, а також видає додаткову інформацію у вигляді імені, ролі (посади) в організації, і перевіряє рівень справжності електронної адреси. Альтернативними інструментами для схожого пошуку є також «voilanorbert.com», а також плагін для браузера «Clearbit Connect».

Якщо є потреба у верифікації адреси електронної пошти, то можна використати веб-інструмент «verifyemailaddress.org». Він працює за принципом перевірки формату адреси електронної пошти, перевірки дійсності доменного імені, перевірки, чи адреса не є одноразовою; також «verifyemailaddress.org» «витягує» MX-записи з доменних рекордів і підключається до поштового сервера (через SMTP, а також імітує відправку повідомлення), щоб переконатися, що поштова скринька дійсно існує для цього користувача/адреси. Деякі поштові сервери не співпрацюють в цьому процесі, в таких випадках результат цього інструменту перевірки електронної пошти може бути не таким точним, як очікувалося. На рисунку 3.15 зображено результат перевірки однієї з адрес, знайдених на минулому кроці.

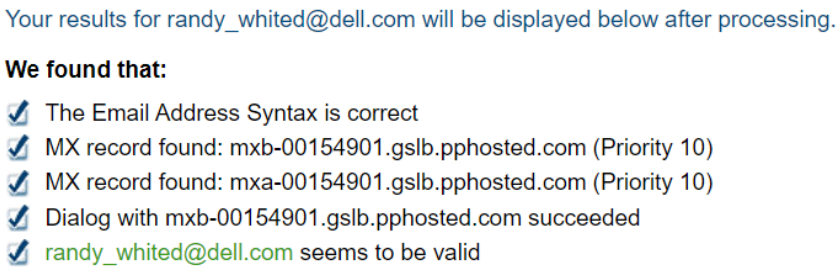

Рисунок 3.15 – Результати перевірки справжності електронної адреси

Наступним кроком безпосередньо є перевірка адреси електронної пошти на присутність у витоках чи порушеннях даних. Для цього можна використати веб-ресурс «haveibeenpwned.com», який аналізує архівовані порушення даних і перевіряє введену адресу на приналежність в них.

Для пошуку була обрана електронна адреса, знайдена на під час OSINT-розвідки, проведеної у минулому пункті, й пов’язана з працівником компанії Dell.

На рисунку 3.16 проілюстровані порушення даних, у яких фігурує електронна адреса «randy_whited@dell.com».

Рисунок 3.16 – Порушення даних на «haveibeenpwned.com»

Отримані результати свідчать про те, що електронна адреса була виявлена у двох порушеннях даних, де типами виявлених даних є електронні адреси, імена, паролі, номери телефонів, геолокації та інші; тобто це задає вектор подальшого пошуку, тому що відомі точні типи даних, які можна буде знайти зловмиснику. Така інформація є цінною з точки зору забезпечення безпеки клієнта в інформаційному просторі, так як дає поштовх і всі можливості для здійснення так званої атаки «credential stuffing» - автоматизоване введення викрадених пар імені користувача та пароля (облікових даних) у форми для входу на веб-сайт з метою шахрайського отримання доступу до облікових записів користувачів.

Якщо відкинути ідею проведення атаки «credential stuffing», можна обмежитися використанням інструментів для пошуку паролів. Для цього буде використаний ресурс «intelx.io», який задіює дані з численних баз даних.

Пошук на «intelx.io» за однією зі знайдених адрес поштової скриньки «randy_whited@dell.com» показує наявність пов'язаних файлів, наборів даних, де розміщена інформація з витоків – рисунок 3.17 [42].

Рисунок 3.17 – Знайдені дані з інструментом «intelx.io»

Із метою отримання паролю, пов'язаного з досліджуваною електронною адресою, був використаний Telegram бот, який шукає за заданим запитом через підключені бази даних паролі – рисунок 3.18.

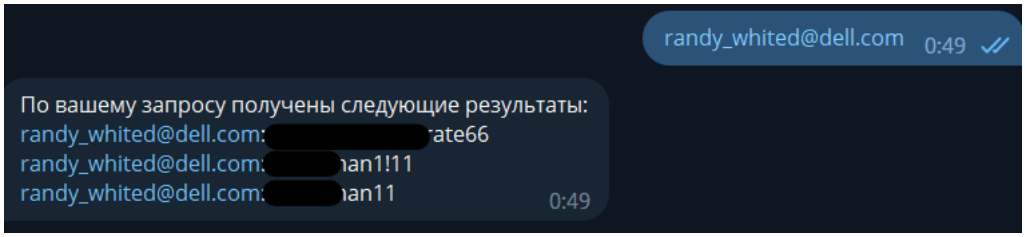

Рисунок 3.18 – Знайдені паролі, пов'язані з цільовою ел. поштою

Таким чином, підсумовуючи дані із попередніх досліджень, можна підсумувати результати. Це буде висвітлено у наступному пункті.

3.3 Виявлення загроз безпеки за розвідданими

У рамках OSINT-дослідження цільової особи, яка є належить до обраної для дослідження компанії, ми знайшли багато типів даних, наведених у таблиці 3.1. Із етичних міркувань, буде висвітлено лише типи знайдених даних без занесення самих даних, хоч дослідження проводилося виключно в навчальних цілях, а збір проходив із відкритих джерел.

Таблиця 3.1 – Типи знайдених розвідданих

№	Тип даних
1	Ім’я
2	Прізвище
3	Робоча адреса електронної пошти
4	Пароль
5	Адреса проживання
6	Колишні адреси проживання
7	Номер телефону
8	Вік
9	Місце роботи
10	Робоча позиція
11	Історія навчання в закладах освіти
12	Досвід роботи
13	Фотоматеріали
14	Вподобання
15	Інформація про зв’язки з іншими особами
16	Благодійні інтереси
17	Facebook
18	Twitter
19	Instagram
20	YouTube

З точки зору безпеки бізнесу така кількість публічно доступної інформації про одного з працівників становить значну загрозу для цільової компанії, а зібрані розвіддані були лише про одну особу.

Загрози для компанії, які можуть становити наявність таких даних у загальнодоступному просторі:

- Проведення фішинг атак. Зловмиснику досить легко знайти адресу ділової електронної пошти працівника, щоб ідентифікувати його посаду й роль у компанії, і виконати спроби фішинг-атаки. Проте якщо він знатиме про ціль ще більше, наприклад, із знайденої загальнодоступної (не приватної) сторінки у соціальних мережах зловмисник «витягне» інформацію про вподобання, зацікавлення жертви, то фішинг атака може бути ефективнішою для зловмисника. До прикладу, якщо б злочинець звернув увагу на благодійні організації, членом яких є W. Randy, то він міг би структурувати й оформити оманливий електронний лист таким чином, щоб замаскуватися саме під цю благодійну організацію, і збільшити особисту релевантність для жертви такого листа. Тоді у жертви буде більше шансів сплутати шахрайську діяльність із законною.

- Впровадження програм-вимагачів (ransomware attacks). Одним з початкових етапів ланцюга програм-вимагачів (ransomware attack kill chain) є розвідка для подальших націлених фішинг атак чи атак, націлених на високопоставлених в компанії осіб (whaling phishing). Це ще один тип загроз, до яких призводить успішна спроба фішинг атак на працівників компанії, коли ті відкривають заражений .exe/.xlss/.pdf/.doc/.zip файл, прикріплений до підробленого листа й заражають систему, потім шифрують файли й викрадають їх, вимагаючи викуп, або переходять за підробленим, наприклад, посиланням для автентифікації на несправжньому сайті Microsoft і вводять свої робочі облікові дані.

- Загроза іміджу компанії. Після успішної атаки й шифрування бандою-вимагачем файлів системи цільової компанії і її відмову сплачувати викуп у грошовому еквіваленті, такі зловмисні угрупування часто публікують абсолютно всі вивантажені й викрадені конфіденційні дані на сторінках DarkNet, які називають «Hall of Shame». Компанія, що стала жертвою такої зловмисної хакерської діяльності, може постраждати з точки зору репутації, тобто наслідком є репутаційні ризики, від яких прямо можуть залежати фінансові прибутки бізнесу.

Окрім вищенаведених загроз безпеки бізнесу, існують й інші. Проте у більшості випадків розвідка OSINT допомагає при оцінці таких ризиків, або навіть їх усуненні, шляхом своєчасного виявлення потрібної інформації про систему

організації. OSINT технології, інтегровані у систему безпеки компанії, здатні покращити як фізичну, так і онлайн-безпеку компаній.

3.4 Висновки до третього розділу

У ході написання третього розділу було реалізовано практичне застосування OSINT-технологій на прикладі цільової приватної компанії.

Був проведений збір інформації про ціль, використовуючи різноманітні загальнодоступні джерела інформації. Також була проведена ідентифікація витоків даних, пов'язаних із цільовою особою, після чого було виявлено загрози бізнесу компанії на основі отриманих розвідданих.

РОЗДІЛ 4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Охорона праці

Розвідка відкритих джерел інформації для виявлення загроз безпеки бізнесу потребує проведення багато робочого часу спеціаліста за комп'ютером, тому необхідно дотримуватись норм роботи для працівників. Норми по охороні праці та техніки безпеки при роботі за електронно-обчислювальною технікою регламентуються НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями» [43], вимогами та нормами державно-санітарної служби при роботі з дисплеями комп'ютерної техніки ДСанПІН 3.3.2.007-98 [44], Санітарними вимогами шуму, інфразвуку та ультразвуку на виробництві ДСН 3.3.6.037-99 [45] та Санітарними мікрокліматичними вимогами до приміщень на виробництві ДСН 3.3.6.042-99 [46].

Безпечна поведінка на виробництві залежить не тільки від професійних знань, навичок і здібностей, а й значною мірою від мотивів поведінки працівника. Відповідно управляти діями людини можна тільки за допомогою управління її мотивами. В обмін за працю працівники очікують не тільки високої оплати, а й створення умов для особистісного росту, отримання задоволення від власної роботи, інших компенсацій, які адекватні професійному рівню та відповідають особистим інтересам.

Ефективна праця допомагає швидшому розвиванню підприємства. Для заохочення працівників потрібно підбадьорення та підтримка з сторони начальства. Стимулювати ефективну роботу можуть матеріальні методи, наприклад премії, винагороди, безкоштовне харчування, додатковий дохід та інше.

Мотиваційний комплекс безпечної поведінки людини носить полі мотивований характер, містить у собі широкий спектр мотиваційних регуляторів як матеріального, так і нематеріального характеру та має певну ієрархічність. Тобто для вирішення охоронних проблем у праці потрібно зацікавити працівників трудитися безпечно не тільки для себе, а й для оточуючих. Очевидно, тільки

закликами, зверненнями, деклараціями, пропагандою ці проблеми навряд чи вдасться вирішити. Потрібно знайти такі способи впливу на людей, щоб вони усвідомили необхідність працювати безпечно у межах яких було б вигідно дотримуватися встановлених регламентів. І цей вплив вона повинна відчувати безпосередньо в процесі всієї трудової діяльності.

Проаналізувавши загальні методи мотивації для підвищення роботи працівників можемо охарактеризувати методи які потрібні для підвищення мотивації безпеки праці осіб на різних підприємствах. Найголовнішим чинником для будь-якого підприємства має бути на першому місці створення безпечних умов праці та дотримання всіх необхідних безпечних заходів для своїх працівників.

Наприклад мікроклімат в приміщенні розробника з електронно-обчислювальною машиною потрібно підтримувати на сталому рівні та відповідно нормам описаним в ДСН 3.3.6.042-99 [37]. При можливості на об’єкті можуть працівники долучитись до охорони праці та запропонувати свої умови, згідно з якими складається договір. У даному договорі вказати свої матеріальні та нематеріальні вимоги. При цьому не може бути системи стимулювання, яка мотивує всіх співробітників однаково. Система стимулів має бути персоніфікованою, ретельно дозованою та розроблятися для кожної людини або певної групи людей з подібними домінуючими потребами, або загальна система має індивідуалізуватися. Тому моніторинг домінуючих потреб персоналу - необхідна умова функціонування мотиваційного механізму. Виходячи з цього, можна визначити види стимулюючих винагород. Вони можуть бути матеріальними, моральними, соціально значимими, морально – психологічними.

Якщо на підприємстві працюють бригади, цехи то корисно буде відзначити їх та видати премію за дотримання усіх вимог щодо безпеки на робочих місцях, без травм чи інших пошкоджень. Також роботодавець або замовник повинен поінформувати працівників під розписку про умови праці та наявність на робочих місцях небезпечних та шкідливих виробничих факторів (фізичних, хімічних, біологічних, психофізіологічних), які виникають під час роботи з екранними пристроями та ще не являються виправленими, а також про можливі наслідки

впливу цих шкідливих факторів на здоров’я працівників відповідно до вимог статті 5 Закону України „Про охорону праці”, тобто робоче місце відповідає ДСанПІН 3.3.2.007- 98 [35].

Якщо на підприємстві працівник виконує роботу у небезпечних для його здоров’я ділянках то йому необхідно надавати надбавку до заробітної плати, адже він ризикує своїм здоров’ям та ставиться до роботи з високою обережністю. Тому роботодавець повинен передбачити за свій рахунок проведення медичних оглядів працівників відповідно до вимог про затвердження Порядку проведення медичних оглядів працівників певних категорій, затвердженого наказом Міністерства охорони здоров'я України від 14 лютого 2012 року № 107, зареєстрованого в Міністерстві юстиції України 23 липня 2007 року за № 846/14113 [36].

Крім матеріального дуже високою цінністю буде моральна підтримка та похвала з сторони керівника, організація відпочинку, екскурсії, влаштування пікніку для робітників які сумлінно дотримувались правил охорони праці. Таким методом не тільки користуються у нашій країні, але і використовують закордонні фірми. До методів для заохочення можемо виділити матеріальні як уже писалось вище, також можуть відноситись моральні тобто подяка у усній чи письмовій формі, відзначення перемоги та інше. Крім методів для заохочення також можуть бути методи покарання за недотримання правил та вимог щодо безпеки охорони праці.

Виходячи з цього, можна використовувати такі методи впливу на мотиви, які стимулюють безпечну поведінку працівників: установити працівникам чітку мету щодо дотримання правил безпеки; створити умови для можливості досягнення цієї мети; визначити винагороду, яку хотіли б отримати працівники. Під час виконання кваліфікаційної роботи з розвідки загроз бізнесу було дотримано усіх вищевказаних норм щодо охорони праці.

4.2 Шкідливий вплив іонізуючого випромінювання

Іонізуючі випромінювання знаходять широке використання в різних галузях промисловості. Їх використовують для автоматичного контролю технологічних

процесів, контролю якості виробів, зварних швів, структури металів тощо [38]. Для виробництва електроенергії на атомних електростанціях необхідне ядерне пальне, виробництво якого, починаючи від добування уранової руди і закінчуючи виготовленням та транспортуванням паливних елементів, призводить до опромінення персоналу. Незначні додаткові дози опромінення працівники отримують від таких техногенних джерел, як теплові електростанції (підвищена активність їх відходів та аерозолів), підприємств, які пов'язані з видобуванням та переробкою корисних копалин, а також різноманітних приладів та обладнання з джерелами випромінювання, що знаходять широке використання у промисловості і сільськогосподарському виробництві. Основним документом, що встановлює радіаційно-гігієнічні регламенти для забезпечення прийнятих рівнів опромінення, є Норми радіаційної безпеки України (НРБУ-97) [39].

НРБУ-97 регламентують опромінення людини джерелами іонізуючого випромінювання в умовах:

– нормальної експлуатації індустріальних джерел іонізуючого випромінювання;

– медичної практики;

– радіаційних аварій;

– опромінення техногенно-підсиленими джерелами природного походження.

Відповідно до цього НРБУ-97 встановлено чотири групи радіаційно-гігієнічних регламентів:

– перша – обмежує опромінення від ядерно-радіаційних об'єктів;

– друга – обмежує опромінення людей від медичних джерел;

– третя – обмежує опромінення в умовах радіаційних аварій;

– четверта – обмежує опромінення від техногенно підсилених джерел природного походження.

Враховуючи різнобічні наслідки опромінення людей іонізуючим випромінюванням, їх нормування здійснюється залежно від категорії людей, що

опромінюються, а також від чутливості органів тіла людини, на які діє іонізуюче випромінювання.

Виділяють наступні категорії:

– особи з числа персоналу, які постійно чи тимчасово працюють безпосередньо з джерелами іонізуючого випромінювання;

– особи з числа персоналу, які безпосередньо не зайняті роботою з джерелами іонізуючого випромінювання, але у зв’язку з розташування робочих місць в приміщеннях та на промислових майданчиках об’єктів з радіаційно ядерними технологіями можуть отримувати додаткове опромінення;

– все населення.

Для осіб категорій А та Б НРБУ-97 [39] встановлюються ліміти річних ефективних доз зовнішнього опромінення, а також ліміти річних еквівалентних доз зовнішнього опромінення окремих органів і тканин людини. Аналогічні ліміти вводяться і для критичних груп осіб категорії В.

Є також обмеження стосовно швидкості накопичення дози для жінок дітородного віку та вагітних жінок, підвищеного опромінення в непередбачуваних ситуаціях та інші. Крім лімітів дози опромінення, встановлюють допустимі рівні (ДР): потужності дози зовнішнього опромінення, забруднення поверхонь, надходження радіонукліду через органи дихання тощо, які визначають виходячи із наведених лімітів дози опромінення. З метою зниження рівнів опромінення населення Міністерство охорони здоров'я України запроваджує рекомендовані рівні медичного опромінення.

Медичне опромінення – це опромінення працівників при медичних обстеженнях чи лікуванні. Опромінення повинно бути обґрунтованим і призначеним тільки лікарем для досягнення корисних діагностичних та терапевтичних ефектів, які неможливо отримати іншими методами діагностики та лікування. Рекомендовані рівні медичного опромінення та детальні вимоги до обмеження і контролю за опроміненням пацієнтів регламентуються окремими спеціальними документами Міністерства охорони здоров'я України. Для радіометричного і дозиметричного контролю використовуються:

– дозиметри – для вимірювання зовнішніх потоків радіоактивного випромінювання;

– радіометри – для вимірювання рівнів забруднення навколишнього середовища; індивідуальні

– дозиметри – для індивідуального контролю.

Серед індивідуальних дозиметрів найбільше розповсюджені прилади, в яких використовують іонізаційні (за величиною іонізації середовища, через яке пройшло випромінювання) та фотографічні (за величиною опромінення фотографічної плівки іонізуючим випромінюванням) методи виміру. У приладах для контролю потужності дози випромінювання широко застосовують іонізаційний та сцинтиляційний методи (за інтенсивністю світлових спалахів, що виникають внаслідок люмінесценції в деяких речовинах під час проходження через них іонізуючих випромінювань).

При роботі з джерелами іонізуючих випромінювань здійснюють контроль і оцінку параметрів радіаційного фактора відповідно до НРБУ-97 [39]. При дотриманні контрольних рівнів умови праці на даному робочому місці оцінюються як допустимі. У разі їх перевищення оцінка шкідливості та небезпечності за радіаційним фактором здійснюється органами Держсанепіднагляду. Засоби та заходи захисту від іонізуючих випромінювань поділяють на організаційні, технічні, санітарно-гігієнічні та лікувально-профілактичні.

Як правило, ефективний захист від іонізуючого випромінювання досягається при одночасному комплексному використанні зазначених заходів та засобів. При їх виборі враховуються особливості джерел випромінювання. Так, основними заходами, направленими на захист від альфа- та бета-випромінювань, є заходи, що націлені на недопущення накопичення альфа- і бета-активних ізотопів в організмі людини та забруднення шкіри: використання спеціального одягу та взуття, протипилових респіраторів, обезпилення повітря, вологе прибирання помешкань, недопущення вживання радіоактивно забруднених харчових продуктів, води та інші.

При роботі з джерелами гама- та рентгенівського випромінювання захист персоналу досягається шляхом зниження активності джерел випромінювання, обмеження часу роботи з ними, збільшення відстані до джерел, екранування джерела іонізуючого випромінювання або зони знаходження людини.

Також у випадку такої радіаційної аварії забруднюється навколишнє середовище, люди можуть отримати травму у вигляді потужної дози опромінення. Призвести аварію на підприємстві може також якщо активна реакційна речовина знаходиться у роботі та це відбувається незаконно. Це може привезти до опромінення жителів та перевищити межу дози опромінення. Частинки з цього випромінювання можуть залишати сліди на дихальній системі на травній системі людського організму. Також ці елементи можуть бути у водних каналах, які постачають питну воду людям.

На підприємстві де проводяться роботи з радіаційними речовинами обов'язково мають вживатись заходи проти радіації. Протирадіаційні захисти це така система правових, організаційних норм та санітарної гігієни. До переліку таких захистів можна включити медичні заходи для забезпечення радіаційної безпеки персоналу та проектно-конструкторські. Для організації заходів проти іонізації опромінювання підприємство має ввести обов'язкові методи щоб подбати про безпеку працюючого персоналу. До таких методів можуть належати заходи які обмежують допуск працівників до джерел які випромінюють радіацію. До таких працівників можемо віднести таких, які не підходять за віком, за статтю та працівники які вже отримали дозу випромінення.

Підприємство мусить створити сприятливі умови що дотримуються встановлених норм та вимог для працівників та застосовувати індивідуальні засоби для захисту працівника цього підприємства. Організація повинна контролювати рівні опромінювання та вести інформаційну систему про стан радіації на підприємстві та призначених місць для праці.

На підприємстві повинні бути проведені заходи щодо організації безпеки для робіт які проводяться у радіаційних ділянках а саме:

– організація роботи нарядів та розпоряджень; -організація та перевірка пропусків до робочих місць;

– оформлення контролю за процесом виконання роботи;

– введення примусового часу на перерву та вчасне закінчення робочого процесу.

До фізичних норм захисту проти радіації існують перешкоди поширення іонізації опромінень. Для поширення дози випромінювання може бути ряд перешкод, залежать вони від кількості годин, перешкоджати може дистанція , також перешкодою може бути чисельність.

Реалізувати заходи проти радіації за певний відрізок часу можливо, тим що працівники , які працюють з іонізованими випромінюванням можуть виконувати вчасно свою роботу, відповідно керівництво може за якісну роботу зменшити кількість робочих днів у тижні. Цим самим вони застереженням вони зменшать знаходження працівників у зоні випромінювання та відповідно буде менше контактування з радіаційними приладами.

Захистити працівників за допомогою відстані підприємство може шляхом доцільного розміщення приміщення, правильно розставити та розрахувати робочі місця для працівників а також забезпечити приладами, які зможуть контактувати, керувати робочим процесом з технікою яка має радіаційний вплив на відстані. Слугувати захистом може покриття свинцем меблів які присутні у приміщенні (двері, вікна, робочі столи), створення перекриття між поверхами та перегородки. Працівникам обов’язково має бути виданий спеціальний одяг ,такі як фартухи, шапочки та рукавиці зшиті з просвинцевої тканини.

Розміщення робочих місць повинно мати правильний розрахунок на загальну кімнату, не робити перенабір та забезпечити відповідним та необхідним обладнанням робочі кабінети.

4.3 Висновки до четвертого розділу

У результаті аналізу вимог щодо охорони праці було визначено, що можна використовувати такі методи впливу на мотиви, які стимулюють безпечну поведінку працівників: установити працівникам чітку мету щодо дотримання правил безпеки; створити умови для можливості досягнення цієї мети; визначити винагороду, яку хотіли б отримати працівники. Під час виконання кваліфікаційної роботи з розвідки загроз бізнесу було дотримано усіх вищевказаних норм щодо охорони праці.

Було описано деталі основного документом, що встановлює радіаційно-гігієнічні регламенти для забезпечення прийнятих рівнів опромінення - Норми радіаційної безпеки України (НРБУ-97).

ВИСНОВКИ

В ході виконанні кваліфікаційної робота освітнього рівня «Магістр» було широко розкрито поняття розвідки на основі відкритих джерел OSINT і описані головні постулати інформації із загальнодоступних джерел та їх видів. Було розкрито тему тенденції використання OSINT-технологій у різних сферах сьогодення.

Приведення детального опису не тільки переваг, але й недоліків застосування OSINT розвідки дозволило скласти загальне бачення щодо ефективності впровадження такої технології задля підтримки безпеки організаціями. Охарактеризовано всі етапи OSINT розслідування покроково, із описом принципів кожного з них. Були охарактеризовані й інші дисципліни збору даних – MASINT, SIGINT, HUMINT, GEOINT, та описано сфери їх застосування сьогодні й у минулому. Висвітлено тему впливу OSINT на міжнародну безпеку, у залежності від міжнародного доступу використання розвідки.

Було проаналізовано всі тактики OSINT й випадки, коли їх можна застосовувати. Розгляд й аналіз конкретних інструментів OSINT надав поняття про специфіку їх роботи й використання задля вирішення задач покращення безпеки. Була проведена ідентифікація існуючих загроз для безпеки бізнесу, при цьому описані особливості застосування OSINT для вирішення цих задач.

Було здійснене практичне застосування OSINT-технологій для цільової приватної компанії: був проведений збір розвідувальної інформації про ціль із використанням інструментів OSINT, після чого були ідентифіковані загрози, із якими може в майбутньому стикнутися компанія.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Isabelle Böhm, Samuel Lolagar (2021) Open Source Intelligence Introduction, legal, and ethical considerations 2(1):1–30.
2. Розвідка на основі відкритих джерел. [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/%D0%A0%D0%BE%D0%B7%D0%B2%D1%96%D0%B4%D0%BA%D0%B0_%D0%BD%D0%B0_%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D1%96_%D0%B2%D1%96%D0%B4%D0%BA%D1%80%D0%B8%D1%82%D0%B8%D1%85_%D0%B4%D0%B6%D0%B5%D1%80%D0%B5%D0%BB.
3. Tomislav Dokman, Tomislav Ivanjko (2019) Open Source Intelligence (OSINT) Issues and Trends 2(1):1–26.
4. Finding Information: Gray Literature. [Електронний ресурс]. URL: https://repository.arizona.edu/bitstream/handle/10150/106108/Types_Gray_Lit.htm.
5. Richelson, Jeffrey (2016) The U.S. Intelligence Community 5(1):1–57.
6. A Brief History of Open Source Intelligence. [Електронний ресурс]. URL: https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/.
7. Heather J. Williams, Ilana Blum (2018) Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise 3(2):1–40.
8. Understanding the Different Types of Intelligence Collection Disciplines. [Електронний ресурс]. URL: https://www.maltego.com/blog/understanding-the-different-types-of-intelligence-collection-disciplines/.
9. Агентурна розвідка. [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/%D0%90%D0%B3%D0%B5%D0%BD%D1%82%D1%83%D1%80%D0%BD%D0%B0_%D1%80%D0%BE%D0%B7%D0%B2%D1%96%D0%B4%D0%BA%D0%B0.
10. H. Akın Ünver (2018) Digital Open Source Intelligence and International Security:: A Primer 2(1):1–30.

11. The Intelligence Cycle: Generating OSINT from OSINF. [Електронний ресурс]. URL: https://www.skopenow.com/news/the-intelligence-cycle-creating-osint-from-osinf.

12. Open Source Intelligence: The Beginners' Guide to OSINT. [Електронний ресурс]. URL: https://www.liferaftinc.com/blog/the-beginners-guide-to-osint.

13. OSINT – Pt.2 – Intelligence Cycle and OSINT Framework. [Електронний ресурс]. URL: https://www.vicarius.io/blog/osint-pt.2-intelligence-cycle-and-osint-framework.

14. Arno H.P. Reuseri (2021) The RIS Open Source Intelligence Cycle 2(1):1–20.

15. Open Source Intelligence Gathering (OSINT). [Електронний ресурс]. URL: https://medium.com/infosec/open-source-intelligence-gathering-osint-f170973ec000.

16. Vinit A. Sinha (2020) Open Source Intelligence and techniques for passive reconnaissance in Linux environment 3(1):1–40.

17. Google hacking. [Електронний ресурс]. URL: https://en.wikipedia.org/wiki/Google_hacking.

18. Search Smarter by Dorking. [Електронний ресурс]. URL: https://kit.exposingtheinvisible.org/en/how/google-dorking.html.

19. What Are Google Dorks? [Електронний ресурс]. URL: https://www.idstrong.com/sentinel/what-are-google-dorks/.

20. Shodan — Computer Search Engine | OSINT Framework #2. [Електронний ресурс]. URL: https://cenabibrahimov.medium.com/shodan-computer-search-engine-osint-framework-2-ed5d9ab0980b.

21. Hack To Learn: OSINT and Passive Reconnaissance. [Електронний ресурс]. URL: https://systemweakness.com/hack-to-learn-osint-and-passive-reconnaissance-efb4cdc2419f.

22. Top 25 OSINT Tools for Penetration Testing. [Електронний ресурс]. URL: https://securitytrails.com/blog/osint-tools.

23. have i been pwned? [Електронний ресурс]. URL: https://haveibeenpwned.com/.

24. OSINT 2021 guide: tools and techniques for threat intelligence. [Електронний ресурс]. URL: https://www.authentic8.com/blog/OSINT-2021-guide-tools-and-techniques.

25. A Guide To Open Source Intelligence (OSINT). [Електронний ресурс]. URL: https://itsec.group/blog-post-osint-guide-part-1.html.

26. Open-source Intelligence (OSINT). [Електронний ресурс]. URL: https://blog.seq.lv/open-source-intelligence-osint/.

27. Defining Active vs. Passive OSINT. [Електронний ресурс]. URL: https://ntrepidcorp.com/managed-attribution/defining-active-vs-passive-osint/.

28. OSINT Tools – Pt.3. [Електронний ресурс]. URL: https://www.vicarius.io/blog/osint-tools-pt.3.

29. The 8 Best OSINT Tools. [Електронний ресурс]. URL: https://www.comparitech.com/net-admin/osint-tools/.

30. OSINT: what it is and what are its tools. [Електронний ресурс]. URL: https://techgameworld.com/osint-what-it-is-and-what-are-its-tools/.

31. Top 14 OSINT tools as of 2021. [Електронний ресурс]. URL: https://www.knowledgenile.com/blogs/top-osint-tools-2021/.

32. 9 Open Source Intelligence (OSINT) Tools for Penetration Testing. [Електронний ресурс]. URL: https://geekflare.com/osint-tools/.

33. Oleksii Kuchmai, Tetiana Shelest (2020) Using open source intelligence (osint) as one of the effective and legitimate ways to avoid threats to the corporation 2(1):1–20.

34. Data Breaches: What They Are, Why They Occur, and How to Prevent Them. [Електронний ресурс]. URL: https://flashpoint.io/blog/what-are-data-breaches-how-to-prevent/.

35. Snovio. [Електронний ресурс]. URL: https://app.snov.io/.

36. LinkedIn. [Електронний ресурс]. URL: https://www.linkedin.com/.

37. Sherlock. [Електронний ресурс]. URL: https://kb.offsec.nl/tools/osint/sherlock/.

38. Facebook. [Електронний ресурс]. URL: https://www.facebook.com/.

39. Instagram. [Електронний ресурс]. URL: https://www.instagram.com/.

40. Spokeo. Know More. [Електронний ресурс]. URL: https://www.spokeo.com/.

41. Phonebook.cz. [Електронний ресурс]. URL: https://phonebook.cz/.

42. Intelligence X. [Електронний ресурс]. URL: https://intelx.io/.

43. Міністерство соціальної політики України, наказ № 207 від 14.02.2018. URL: https://zakon.rada.gov.ua/laws/show/z0508-18#Text.

44. ДСанПІН 3.3.2.007-98 № 7 від 10.12.98. URL: https://zakon.rada.gov.ua/rada/show/v0007282-98#Text.

45. ДСН 3.3.6.037–99. Санітарні норми виробничого шуму, ультразвуку та інфразвуку. URL: https://zakon.rada.gov.ua/rada/show/va037282-99#Text.

46. Постанова 01.12.99 № 42 «Санітарні норми мікроклімату виробничих приміщень ДСН 3.3.6.042-99». URL: https://zakon.rada.gov.ua/rada/show/va042282-99#Text.

47. Методичні рекомендації для проведення атестації робочих місць за умовами

48. праці. Затверджено міністром праці України 1.09.1992 р, постанова № 41. URL: https://zakon.rada.gov.ua/rada/show/v0041205-92#Text.

49. Наказ від 14.07.97 № 208 «Про затвердження Норм радіаційної безпеки України (НРБУ-97)». URL: https://zakon.rada.gov.ua/rada/show/v0208282-97#Text.

Додаток А – Тези конференції

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

X НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

7–8 грудня 2022 року

ТЕРНОПІЛЬ
2022

УДК 004.056
К. Николин
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗВІДКА ВІДКРИТИХ ДЖЕРЕЛ ІНФОРМАЦІЇ ДЛЯ ВИЯВЛЕННЯ ЗАГРОЗ БЕЗПЕКИ БІЗНЕСУ

K. Nykolyn

OPEN SOURCE INTELLIGENCE FOR IDENTIFYING BUSINESS SECURITY THREATS

Світові підприємства працюють в епоху цифрової трансформації. Це дає безліч переваг для компаній: допомагає покращити клієнтський досвід, продуктивність й управління ресурсами. Але разом із цими перевагами, більш широке впровадження технологій також означає збільшення можливості компрометації даних.

Open-source intelligence (OSINT) – розвідка на основі аналізу відкритих джерел інформації) – одна з форм процесу організації та управління збором розвідувальних даних (Intelligence Collection Management), що включає їх пошук і відбір із публічних загальнодоступних джерел, добування та аналіз інформації, формування розвідувального документу для прийняття відповідного рішення [1]. Процес OSINT складається зі збору, обробки, аналізу даних та формування звіту після їх виявлення. У світі кібербезпеки OSINT найчастіше використовується на ранніх стадіях тестування на проникнення, при цьому ця інформація також доступна і суб'єктам загроз; етап розвідки забезпечує базу для пошуку вразливостей для експлуатації з технічної точки зору. Кожна організація має модифіковану структуру OSINT відповідно до своєї мети, оскільки вимоги до OSINT відрізняються від однієї організації до іншої. Проте OSINT є лише однією з усталених дисциплін збору розвідувальної інформації. Стандартного переліку дисциплін збору розвідувальної інформації не існує, однак у розвідувальному співтоваристві США існує консенсус щодо існування п'яти основних дисциплін: HUMINT, SIGINT, IMINT/GEOINT, MASINT [2], і звичайно OSINT. Варто зазначити, що деякі з цих дисциплін (або їх піддисциплін) використовуються виключно державними установами, особливо у сфері воєнної та спеціальної розвідки.

Приватні компанії головним чином розглядають застосування сучасних інструментів OSINT як ефективний спосіб ідентифікації зовнішньої інформації та виявлення внутрішніх активів, що перебувають у відкритому доступі.

У подальших дослідженнях розглядатиметься саме розвідка на основі відкритих джерел – OSINT, адже застосування даного методу може допомагати організаціям зменшити бізнес-ризики й фінансові втрати шляхом збору даних у видимій частині Інтернету й у даркнеті, моніторити у реальному часі інформацію щодо можливих атак, ідентифікувати певні внутрішні загрози компанії.

Література

1. Електронна енциклопедія Wikipedia. Англомовна версія. URL: http://en.wikipedia.org/wiki/Open-source_intelligence
2. Intelligence Studies: Types of Intelligence Collection. URL: https://usnwc.libguides.com/c.php?g=494120&p=3381426.