УДК 004.056
Піківець Г.М.[1], Корольков Р.Ю.[2]
[1] студ. гр. БКз-813м НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

ОГЛЯД МЕТОДІВ OSINT ТА ЇХ РОЛЬ У РОЗСЛІДУВАННІ КІБЕРІНЦИДЕНТІВ

Кіберзлочинність стрімко еволюціонує, перетворюючись на одну з найбільш актуальних проблем сучасності. Зловмисники постійно удосконалюють свої методи, завдаючи шкоду як приватним особам, так і великим компаніям. У цьому контексті, розслідування кіберінцидентів стає все більш важливим завданням, оскільки від його успіху залежить не лише компенсація завданих збитків, але й запобігання майбутнім атакам.

Звичайні методи розслідування не завжди є ефективними у віртуальному просторі, де зловмисники використовують складні інструменти та методи для приховування своїх дій. Розвідка з відкритих джерел стає все більш ефективним інструментом у боротьбі з кіберзлочинністю та кіберінцидентами [1]. В контексті протидії кіберзлочинності методи розвідки з відкритих джерел набувають все більшого значення, що дозволяє збирати інформацію про зловмисників, їхні методи та цілі, а також моніторити кіберзагрози.

Open Source Intelligence (OSINT) – це концепція, методологія та технологія для отримання та використання військової, політичної, економічної та іншої інформації з відкритих джерел без порушення чинного законодавства. OSINT використовується для прийняття рішень у сфері національної оборони та безпеки, у розслідуваннях кіберзлочинів, терористичних актів та інших подій, що включає збір інформації, реєстрацію, облік та аналіз, аналітичну та синтетичну обробку первинної інформації, зберігання та поширення інформації, інформаційну безпеку та подання результатів дослідження. Після того, як первинна інформація з відкритих джерел пройде аналіз та обробку, вона може стати корисною і ,якщо ця інформація не відноситься до категорії, що є державною таємницею, вона може бути розголошена [2].

Щоб максимізувати ефективність OSINT, вкрай важливо застосовувати різноманітні методи та використовувати відповідні інструменти. Ці техніки можна умовно розділити на пасивні та активні [3].

Пасивні OSINT-методи передбачають збір інформації без безпосереднього звернення до джерел, використовуючи інформацію, доступну для загального ознайомлення.

Деякі поширені методи включають:

1. Аналіз соціальних мереж: Facebook, Twitter, LinkedIn, Instagram та інші. Аналізуючи профілі користувачів, публікації та зв'язки, аналітики можуть отримати цінну інформацію про людей, організації та тенденції.

2. Запити в пошукових системах Google, Bing, DuckDuckGo та інших. Використовуючи оператори розширеного пошуку такі як Google Dork можливо уточнювати пошуки та отримувати цільову інформацію.

3. Дослідження веб-сайтів і доменів є важливою частиною методів OSINT і може надати цінну інформацію про підприємства, організації чи навіть окремих користувачів. Такі методи, як записи WHOIS, аналіз IP-адрес і веб-скрапінг, можуть розкрити важливу інформацію.

Активні методи OSINT передбачають безпосередню взаємодію з джерелами та активний збір даних, а також вимагають від користувача значних зусиль, в тому числі фінансових витрат.

До таких методів належать:

1. Сканування веб-сайтів та індексація каталогів що включає безпосередню взаємодію з веб-сайтами шляхом сканування їх структури, пошуку вразливостей та визначення характеристик, таких як доступні служби чи ресурси.

2. Звернення до джерел із запитами про інформацію ВКЛЮЧАЮЧИ направлення запитів до компаній, організацій або громадських установ для отримання конкретної інформації.

3. Активне спостереження і взаємодія в соціальних мережах. Цей підхід передбачає безпосереднє спостереження за активністю користувачів у соціальних мережах та взаємодію з ними для отримання додаткової інформації.

4. Тестування на проникнення та збір інформації про безпеку мережі передбачає активне тестування систем та мереж на предмет наявності потенційних вразливостей шляхом спроби проникнення в них.

5. Дослідження публічних архівів, таких як судові документи, реєстрація бізнесу та майнові записи, що надають цінну інформацію про окремих осіб, організації та їх діяльність.

6. Аналіз зображень і відео, що часто містять цінну інформацію, яка може сприяти збору розвідувальних даних. Такі методи, як реверсивний пошук зображень, аналіз метаданих і відеокриміналістика, допомагають отримати інформацію з візуального вмісту.

У розслідуванні кіберінцидентів OSINT відіграє важливу роль, допомагаючи: ідентифікувати зловмисників; визначити інструменти та методи які використовуються зловмисниками, та способи захисту від них; зібрати докази; моніторити кіберзагрози.

Хоча OSINT є потужним інструментом для розслідування кіберзлочинів та забезпечення кібербезпеки, його використання вимагає уважного

врахування етичних аспектів. Якість отриманих даних не завжди є достатньою, що потребує критичного аналізу та перевірки. Крім того, використання Open Source Intelligence може порушувати юридичні обмеження, особливо у випадках, коли стосується конфіденційної інформації або національної безпеки. Отже, при використанні OSINT необхідно дотримуватися етичних принципів та враховувати можливі ризики і обмеження, щоб забезпечити ефективність та законність проведених дій [4].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Мамедова Л.Ш. Особливості використання спеціальних знань під час розслідування кіберзлочинів: міжнародний досвід. Юридичний науковий електронний журнал. 2021. № 12. С. 392–395. URL: https://doi.org/10.32782/2524-0374/2021-12/99 (дата звернення: 09.04.2024).

2. Електронна енциклопедія Wikipedia. Українськомовна версія URL: https://uk.wikipedia.org/w/index.php?title=Розвідка_на_основі_відкритих_джерел&stable=0 (дата звернення: 09.04.2024)

3. THE OSINT FRAMEWORK: UNVEILING THE ART OF INFORMATION GATHERING URL: https://www.pvt365.net/the-osint-framework-unveiling-the-art-of-information-gathering (дата звернення: 09.04.2024).

4. Open Source Intelligence (OSINT): A Powerful Tool for Information Gathering URL: https://www.linkedin.com/pulse/open-source-intelligence-osint-powerful-tool-information-t-w96pc (дата звернення: 09.04.2024)