

Гриненко Юлія Ігорівна,
*PhD, старший аналітик,
Бюро економічної безпеки України,
м. Київ, Україна*

ВИКОРИСТАННЯ OSINT-ІНСТРУМЕНТІВ В АУДИТІ

Одним з ключових інструментів, який використовують під час виявлення та збору даних, є відкрите джерело розвідки (OSINT). **OSINT (аналітика з відкритим вихідним кодом)** це тип збору даних, який включає в себе збір та аналіз загальнодоступної інформації для підтримки різних видів аналізу [1].

В контексті аудиту OSINT може використовуватися для виявлення потенційних загроз, оцінки ефективності заходів безпеки та виявлення вразливостей в системах чи мережах. Особливо це стосується виявленню ризиків пов'язаних з протидією терористичним організаціям, незаконному відмиванню та легалізації грошей отриманих злочинним шляхом [2].

Історію OSINT можна простежити до середини 20-го століття, коли розвідувальні служби почали використовувати загальнодоступну інформацію на додаток до своїх традиційних джерел даних. У 1990-х роках Інтернет і широка доступність цифрової інформації значно розширили сферу застосування та потенціал OSINT. З розвитком соціальних мереж та інших онлайн-платформ OSINT стає все більш важливим інструментом для широкого кола організацій, у тому числі в області фінансової безпеки.

Сьогодні OSINT може стати важливим компонентом багатьох стратегій аудиту, надаючи цінну інформацію про потенційні загрози безпеки, вразливості та інші ризики. Інструменти OSINT можливо використовувати для перевірки контрагентів, встановлення пов'язаних осіб та кінцевих бенефіціарів. Зокрема, особливо важливою для аудиту є інформація про офшорні компанії, справжніх власників, залучення компанії-партнера до тіньових схем.

Методи OSINT можуть включати пошук по онлайн-баз даних та платформ соціальних мереж, моніторинг загальнодоступного мережевого трафіку. Аналізуючи цю інформацію, можна отримати уявлення про потенційні ризики, виявити виникаючі загрози і поліпшити загальний стан безпеки підприємства. До основних методів збору OSINT належать:

1. Пошук в Інтернеті - Використання пошукових систем, таких як Google або Bing, для виявлення інформації, що відноситься до певної теми, включаючи інформацію про потенційні загрози. Може включати в себе проведення сканування портів, збір даних про доменні імена і IP-адреси, а також аналіз мережевого трафіку.

2. Моніторинг соціальних мереж - Моніторинг платформ соціальних мереж для виявлення потенційних загроз, відстеження суспільних настроїв та збору інформації про окремих осіб або організацій. Включає в себе збір та аналіз інформації з платформ соціальних мереж, таких як Twitter, LinkedIn і Facebook.

3. Моніторинг темної мережі - Моніторинг темної мережі для виявлення

потенційних загроз, відстеження незаконної діяльності та збору даних про злочинних організаціях. Включає в себе моніторинг і аналіз інформації в темній мережі, яка є частиною Інтернету, яка не індексується пошуковими системами і часто використовується для незаконної діяльності.

4. Запити на публічні записи - Запитувати публічні записи у державних установ і інших організацій для отримання інформації про приватних осіб або організаціях. Включає в себе збір та аналіз інформації з законних джерел, таких як судові протоколи, урядові звіти і публічні документи. Legal OSINT може використовуватися для збору даних про приватних осіб чи організації, виявлення потенційних юридичних ризиків і контролю за дотриманням нормативних вимог.

5. Групи обміну інформацією - Участь у групах з обміну інформацією, таких як ISACs (Центри обміну інформацією та аналізу), для обміну інформацією та даними про потенційні загрози та вразливості.

6. Автоматизовані інструменти - Використання автоматизованих інструментів, таких як пошукові системи і інструменти інтелектуального аналізу даних, для збору та аналізу великих обсягів даних з різних джерел.

Основний підхід до використання OSINT полягає у зборі інформації з відкритих джерел, таких як соціальні мережі, блоги, форуми, новинні сайти та інші джерела. Крім того, використовуються спеціальні інструменти для збору інформації, такі як сканери веб-сайтів та соціальних мереж. До основних інструментів OSINT можна віднести:

1. Maltego: Широко використовуваний інструмент для збору та аналізу даних з відкритим вихідним кодом, Maltego дозволяє користувачам візуалізувати дані і взаємозв'язку, щоб допомогти виявити потенційні загрози та вразливості.

2. Recon-ng: Потужний інструмент OSINT, Recon-ng може використовуватися для збору інформації з широкого спектру джерел, включаючи пошукові системи, платформи соціальних мереж і загальнодоступні запису.

3. theHarvester: Інструмент OSINT для пошуку електронної пошти та доменних імен, theHarvester може використовуватися для збору інформації про потенційних цілях, включаючи адреси електронної пошти, піддомени і пов'язані домени.

4. FOCA: Інструмент для аналізу метаданих, FOCA може використовуватися для виявлення і вилучення прихованих метаданих документів та інших файлів для підтримки збору та аналізу розвідувальних даних.

5. OSINT Framework: Набір різних інструментів і ресурсів OSINT, платформа OSINT надає повний набір інструментів і ресурсів для проведення збору розвідданих з відкритим вихідним кодом.

6. Creepy: Інструмент OSINT для геолокації, Creepy може використовуватися для відстеження та відображення онлайн-активності окремих осіб або організацій на основі їх соціальних мереж та іншого онлайн-активності.

7. Intelligence X: Інтелектуальна пошукова система Intelligence X може використовуватися для пошуку інформації про приватних осіб, організаціях і доменах з широкого спектру джерел.

8. Google Dorks: Ряд операторів розширеного пошуку Google Search, Google

Dorks можна використовувати для пошуку інформації і вразливостей, які можуть бути недоступні для перегляду з допомогою стандартних пошукових запитів.

OSINT також включає в себе аналіз отриманої інформації. Проаналізувавши відомості, зібрані з різних джерел, аудитори отримують більш повну картину щодо діяльності підприємства та посадових осіб. Цей аналіз включає зіставлення інформації з різних джерел, аналіз тенденцій та патернів.

Збір та аналіз великих об'ємів інформації в режимі реального часу є важливим етапом роботи. Використання відкритих даних - це один з інструментів, який дозволяє аудиторам збирати та аналізувати відкриту інформацію, для виявлення та розшуку потенційних ризиків при проведенні аудиту фінансової звітності чи узгоджених процедур.

Одним з найпоширеніших методів OSINT – є пошук інформації за Email Address, Domain Name та IP Address. Ці методи дозволяють виявити зв'язки та співвідношення між людьми, компаніями, організаціями та різними доменами та IP-адресами, що допомагає зрозуміти, які активи, контрагенти чи операції можуть бути пов'язані з потенційними ризиками.

Для пошуку інформації за Email Address аудитори можуть використовувати різноманітні інтернет-ресурси та сервіси, такі як Hunter, Whois, Pipl, Spokeo, що дозволяють знайти додаткові електронні адреси, пов'язані з конкретним користувачем, а також інформацію про компанії, з якими він пов'язаний.

Щодо пошуку інформації за Domain Name, аудитори можуть використовувати сервіси Whois та DomainTools. Ці інструменти роблять детальний аналіз доменного імені, включаючи інформацію про власника, дату реєстрації, контактну інформацію та інші важливі дані, які можуть допомогти зрозуміти, які активи пов'язані з власником домену.

Пошук інформації по IP Address дозволяє виявити місцезнаходження та власника конкретної IP-адреси. Аудитори можуть використовувати сервіси MaxMind та IP2Location для отримання інформації про власника IP-адреси, тим самим примножують ймовірність ідентифікації пов'язаних з ним контрагентів.

Отже, використання відкритих даних та методів OSINT-розслідування в роботі аудиторської діяльності є важливим інструментом для виявлення загроз та ризиків при проведенні аудиту фінансової звітності.

Список використаних джерел:

1. NATO Open Source Intelligence Handbook URL: http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf
2. Cyber Intelligence by Europol URL: <https://www.europol.europa.eu/activities-services/services-support/intelligence-analysis/cyber-intelligence>.
3. Williams, H., & Blum, I. (2018). *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*. *Defining Second Generation Open Source Intelligence (Osint) for the Defense Enterprise*. URL: <https://doi.org/10.7249/rr1964>