УДК 004.056

Б. Д. Панченко

СИСТЕМА АВТОМАТИЗОВАНОЇ РОЗВІДКИ З ВІДКРИТИХ ДЖЕРЕЛ ІНФОРМАЦІЇ

Вінницький національний технічний університет

Анотація

Розглянуто проблеми, що призвели до необхідності використання системи автоматизованої розвідки, та розглянуто реалізації схожих засобів.

Ключові слова: розвідка відкритих джерел, *державні реєстри, відкриті дані.*

Abstract

The problems that led to the need to use an automated intelligence system are considered, and the implementation of similar tools is considered.

Keywords: open source intelligence, state registers, open data.

Вступ

Оскільки кожна людина, організація і під'єднаний до інтернету пристрій залишає в мережі свій інформаційний слід, велику частину цих даних можна знайти за допомогою легальних інструментів, що є у відкритому доступі. Здійснення автоматизованої розвідки допомагає знайти загальнодоступну інформацію про працівників, внутрішню діяльність компанії, а також дані за її межами. Іноді конфіденційна інформація міститься в метаданих, які організація випадково опублікувала. Таким чином, аналіз інформації, що знаходиться у відкритому доступі може використовуватись і зловмисниками для проведення атак і спеціалістами з кібербезпеки для запобігання таких атак.

Результати дослідження

Люди є найважливішою частиною організації, але вони також можуть бути її слабкою ланкою з позиції кібербезпеки. Згідно з деякими з останніх досліджень станом на 2021 рік до 34% всіх організацій щорічно піддаються впливу інсайдерських атак [1].

OSINT має чітко визначену та точну методологію. З науково-технічної точки зору, особливо цікавими є його три основні етапи.

Першим є етап збору, на якому загальнодоступні дані відбираються з відкритих джерел відповідно до цілі або мети. Зокрема, Інтернет є одним з найкращих джерел інформації завдяки обсягу наявного матеріалу та легкодоступності. Процес збору особливо важливий, тому що з цього етапу запускається весь процес формування розвідки [2].

Потім, на етапі аналізу, зібрана інформація обробляється для отримання цінної та зрозумілої інформації. Дані самі по собі не є корисними, тому їх слід інтерпретувати, щоб отримати перші факти, отримані з поглибленого аналізу [2].

Нарешті, у процесі вилучення знань інформація, оброблена раніше, береться як основа для більш складних алгоритмів висновків. Таким чином можна виявляти певні закономірності, поведінку профілю, прогнозувати значення або співвідносити події [2].

Використовуючи отриману з цих джерел інформацію, OSINT постійно розширює обсяг даних про ціль. Таким чином, знайдена інформація знову стимулює процес збору [3].

Оскільки для здійснення розвідки з ціллю запобігання атак у кіберпросторі необхідна інформація з відкритих джерел даних, необхідно створити для них критерії оцінки з метою покращення результатів пошуку інформації, та збільшення її якісних показників, що в результаті збільшить ефективність використання системи спеціалістами з кібербезпеки.

Те, що книга, стаття чи веб-сайт відповідають критеріям пошуку, не означає, що вони є надійним та достовірним джерелом інформації.

Для того, щоб підвищити рівень отримуваних при розвідці результатів, необхідно розробити критерії оцінювання інформативності, негативності та надійності джерел перед їх додаванням в базу, та користуватись останніми нововведеннями, що стосуються відкритих даних у державі.

Одними з найбільш результативних джерел відкритих даних є пошукові системи та соціальні

мережі, тому було розглянуто використання пошукових мереж у якості джерела відкритих даних, проаналізовано основні фільтри пошукових мереж та здійснено розподіл соціальних мереж за рядом ознак, таких як призначення, та потенціальні дані для OSINT. Незважаючи на об’єм отримуваних даних, їх не можна з впевненістю вважати достовірними, тому їх буде включено до неперевірених джерел даних.

Після проведення аналізу програмних засобів було виявлено, що незважаючи на широке застосування міжнародних соціальних мереж та ресурсів у якості інформаційних джерел, засоби часто зовсім не використовують відкриті реєстри України, що є суттєвим недоліком при формуванні результату розвідки.

Висновок

Отже, за допомогою удосконаленної системи автоматизованої розвідки вирішується ряд недоліків програм аналогів, таких, як включення недостовірних результатів та відсутність диференціації результатів за негативнстю з метою покращення роботи спеціалістів з кібербезпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 21+ Insider Threat Statistics to Look Out For in 2021. [Електронний ресурс]. –Режим доступу: URL https://techjury.net/blog/insider-threat-statistics/#gref – Назва з екрану.

2. Gibson H. Acquisition and preparation of data for OSINT investigations //Open Source Intelligence Investigation. – Springer, Cham, 2016. – С. 69-93.

3. H. J. Williams and I. Blum, "Defining second generation open source intelligence (OSINT) for the defense enterprise", 2018.

Панченко Богдан Дмитрович — студент групи 1БС-20м, факультет інформаційних технологій, Вінницький національний технічний університет, Вінниця, e-mail : r7m250@gmail.com

Bohdan Panchenko — student, Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: r7m250@gmail.com