Напрям № 2
Актуальні питання здійснення правоохоронної діяльності, забезпечення публічного порядку та безпеки в умовах дії воєнного стану

Olha Haborets
PhD in Pedagogical Sciences, Associate Professor of the Department of Operational-search Activities and Information Security of Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine

Olha Lunhol
PhD in Pedagogical Sciences, Associate Professor of the Department of Operational-search Activities and Information Security of Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine

METHODS OF USING OSINT IN CYBERPOLICE ACTIVITIES

OSINT, or Open Source Intelligence, refers to information that is publicly available and can be obtained from sources such as the internet, social media, news articles, and public records. OSINT is a valuable resource for intelligence gathering and can be used by various organizations, including law enforcement agencies, to support their investigations.

OSINT can provide a wide range of information, including individuals' personal and professional details, organizations' operations, and global events. OSINT is often used in the field of cybersecurity to identify potential cyber threats and vulnerabilities. OSINT is also used in business intelligence to gather information on competitors, industry trends, and market opportunities.

The use of OSINT requires specialized skills and tools, including search engines, data mining software, and analytical techniques. OSINT can be a valuable resource for intelligence gathering, but it is important to ensure that the information obtained is accurate, relevant, and reliable. OSINT should also be used ethically and in compliance with applicable laws and regulations.

Here are some methods of using OSINT in cyber police activities:

Social Media Monitoring: Cyber police can monitor social media platforms to gather information on individuals or groups suspected of cybercrimes. Social media monitoring can also help in identifying potential threats and suspicious activities.

Dark Web Monitoring: The dark web is a hidden network of websites not accessible through traditional search engines. Cyber police can use OSINT tools to monitor the dark web to identify criminal activities such as cybercrime forums, hacking services, and illegal marketplaces.

E-mail Header Analysis: OSINT tools can be used to analyze the headers of e-mail messages to track the source and location of the sender. This can be useful in tracking cybercriminals who use email as a means of communication.

IP Address Tracking: Cyber police can use OSINT tools to track the IP addresses of suspects and identify their geographical location. This can be helpful in identifying the source of cyber-attacks and tracing the origin of malicious activities.

Geolocation Tracking: OSINT tools can be used to track the location of mobile devices and identify the whereabouts of suspects. This can be useful in locating cybercriminals who use mobile devices to conduct their activities.

Website Analysis: Cyber police can use OSINT tools to analyze websites and identify malicious activities such as phishing scams, malware, and ransomware. Website analysis can also help in identifying the owners of suspicious websites.

Online Reputation Management: OSINT tools can be used to monitor the online reputation of individuals and organizations suspected of cybercrimes. This can help in identifying suspicious activities and detecting attempts to hide incriminating information.

A feature of OSINT is that it is always specific information, collected and structured in a special way to answer specific questions [2]. Its advantages include the availability of various sources of information, as well as the volume of its arrays, versatility of information, a large number of existing techniques, methods and technologies. The end result of OSINT is always some knowledge obtained as a result of conclusions from the information received [3].

OSINT technology is actively used by Cobwebs Technologies [4]. They developed an AI-powered web investigative platform. Analytical data is collected in real time, the investigation is carried out automatically. Cobwebs solutions are used in corporate security, financial institutions, law enforcement structures, public and national security.

In conclusion, OSINT is a powerful tool that can be used by cyber police to investigate and prevent cybercrimes. By leveraging OSINT tools, cyber police can gather intelligence, track suspects, and identify potential threats, leading to more effective and efficient law enforcement.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Gill R. What is Open-Source Intelligence? SANS. URL: https://www.sans.org/blog/what-is-open-source-intelligence/ (Дата звернення: 15.03.2023).

2. Щурат Т.Г. Деякі аспекти розвідки з відкритих джерел інформації (OSINT) / Т.Г. Щурат, А.О. Смук // Оперативно-розшукова діяльність Національної поліції: проблеми теорії та практики: Всеукраїнська науково-практична конференція (20 жовтня 2017 р.). – м. Дніпро: ДДУВС, 2017. – С.126- 128. URL: http://dspace.oduvs.edu.ua/handle/123456789/654 (дата звернення: 18.03.2023).

3. Уфімцева О. Використання OSINT в умовах збройної агресії рф проти України. URL: http://surl.li/foype (дата звернення: 19.03.2023).

4. OSINT: технологія збору та аналізу даних з відкритих джерел. Софтлист. URL: https://ua.softlist.com.ua/articles/osint-tekhnologiya-sbora-i-analiza-dannyh-iz-otkrytyh-istochnikov/ (дата звернення: 19.03.2023).