Список використаних джерел:

1. Боднар І. Р. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. 2014. № 1. С. 68–75.
2. Панченко О. Інформаційна складова національної безпеки. Вісник Національної академії Державної прикордонної служби України. 2019. Випуск 3. URL: https://www.rdc.org.ua/download/stati/Informational-warehouse.pdf (дата звернення: 15.04.2024).
3. Паш Б. В. Складові інформаційної безпеки держави: постановка питання. Закарпатські правові читання. 2017. Том 1. С. 509–512.
4. Кобко Є. В. Інформаційна безпека в системі національної безпеки: сучасність і перспективи. National law journal: teory and practice. 2019. March. С. 46–50.
5. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий електронний журнал. 2020. № 2. С. 200–203.
6. Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС і навчальному процесі : збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичної конференції 23 грудня 2016 року / упорядник Т. В. Магеровська /. Львів : ЛьвДУВС, 2017. 313 с.

Haborets Olha Andriivna
PhD, Associate Professor of the Department of Operational-search Activities and Information Security of Donetsk State University of Internal Affairs

OSINT: A SCIENTIFIC APPROACH TO INFORMED DECISION-MAKING

In the current era of rapid technological progress and widespread internet availability, Open Source Intelligence (OSINT) technologies hold significant sway over the sourcing, analysis, and utilization of information. This dominance stems from their capacity to systematically navigate the vast expanse of digital data, extracting valuable insights crucial for informed decision-making across various domains.

OSINT entails the systematic gathering, examination, and utilization of publicly available information from diverse sources to draw meaningful conclusions and comprehend various situations. This methodology finds application across intelligence, cybersecurity, competitive analysis, law enforcement, and other sectors where access to open information enhances decision-making processes. It relies on sources like social media, public databases, websites, and forums.

Within the domain of OSINT, researchers and analysts harness specialized tools and techniques to collect, assess, and interpret vast amounts of data, thereby extracting

valuable insights [1, p. 92]. This process encompasses revealing information about individuals, companies, organizations, events, technologies, and other pertinent subjects.

However, due to the multifaceted nature of OSINT and the array of associated tools, our focus narrows to a specific aspect within this expansive field - the OSINT Framework. This framework comprises tools and resources tailored to gather and analyze information from publicly available internet sources, facilitating exploration, monitoring, and analysis of various data types to identify patterns, trends, and potential threats. Leveraging OSINT proves indispensable across diverse domains such as cybersecurity, fraud prevention, criminal investigations, incident analysis, and intelligence operations. The abundance of openly accessible internet data provides valuable insights into pinpointing threats, vulnerabilities, suspicious activities, and emerging trends, benefiting both commercial and public sectors by supporting decision-making, compiling statistics, monitoring social media, and gauging public sentiment.

Effectively employing OSINT requires adept skills in information searching, filtering, and analysis, alongside adherence to legal and ethical considerations regarding open information access. This article serves as a valuable resource compilation for newcomers to the OSINT and infosec fields, while seasoned professionals will find it enriching with useful information and unique materials.

Open Source Intelligence involves utilizing publicly available sources to acquire and assess information accessible to the general public, with the primary aim of comprehending given situations or entities through processing and analyzing openly accessible data. With technological advancements and data proliferation, OSINT offers extensive application opportunities across various domains.

In the realm of social networks and media, OSINT encompasses activities such as monitoring social media platforms for interactions, community dynamics, and key individuals, as well as tracking news and content from diverse sources to grasp the prevailing situation.

In geospatial analysis, OSINT utilizes geodata including satellite imagery and geographic information systems to locate objects and scrutinize spatial relationships, while textual and visual information analysis involves employing natural language processing (NLP) algorithms and computer vision technologies.

Integral to OSINT are data analysis platforms like Maltego and Recorded Future, along with ethnographic analysis focusing on sociocultural learning to understand behavioral patterns and cultural differences for effective information contextualization.

These OSINT tools find applications across security, intelligence, business intelligence, and more, incorporating scientific methodologies and technologies to optimize data collection and analysis, thereby facilitating well-informed decision-making processes.

References:

1. Zhmur N.V. Mezhdunarodno-pravovye standarty zashhity informacii: otdelnye aspekty. Legeasi Viata. 2014. № 2/2 (266). S. 90-93.