УДК 004.6

ALGORITHM OF USING THE OSINT TECHNOLOGY IN MODERN SERVICES

Bukatyi Y.I[1]., Bukatyi D.I.[2], Zhovtiak N.O.[3], Storchak A.S.[4]

Institute of Special Communications and Information Protection of National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.
ORCID: [1]https://orcid.org/0009-0004-0201-8965, [2]https://orcid.org/0009-0003-2670-1382, [3]https://orcid.org/0009-0005-3773-5232, [4]https://orcid.org/0000-0002-5267-3122
E-mail: [1]eg.bukatij@gmail.com, [3]bukatyjdana@gmail.com, [3]nazarlisni2606@gmail.com, [4]storchakanton@gmail.com.

Copyright © 2023 by author and the journal “Automation of technological and business – processes”.
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licanses/by/4.0

DOI: 10.15673/atbp.v15i1.2492

Abstract. *The tools and forms of the process of organizing and managing the collection of intelligence data are considered. The relationship between operations with different types of information is shown. Techniques of active and passive information collection were studied. The main types of OSINT data collection tools, their capabilities and application features are given. The classification of resources for OSINT operations is given. An information search algorithm using modern services (entertainment services) has been developed. The proposed algorithm for using OSINT technology in modern services allows you to obtain the maximum amount of data, minimize resources and time, and takes into account the peculiarities of the legislation of the country of the OSINT object. Based on the statement, the article also discusses the relationship between different types of information, the capabilities and application features of various OSINT data collection tools, and the classification of resources for OSINT operations. Additionally, it presents an information search algorithm that utilizes modern services, considering the peculiarities of the legislation of the country of the OSINT object.*

Keywords: *OSINT tools, algorithm, open source information, intelligence collection , data.*

1. Introduction

Open Source Intelligence (OSINT) is a method of gathering information from public or other open sources, which can be used by security experts, national intelligence agencies, or cybercriminals. When used by cyber defenders, the goal is to discover publicly available information related to their organization that could be used by attackers, and take steps to prevent those future attacks.

A major source of intelligence that cannot be overlooked is the vast amount of publicly available information (PAI) being produced by consumers, hackers, newsmakers, and bloggers every single day. Globally, almost every person and organization is communicating across multiple platforms and networks, as well as handling personal and corporate needs virtually – such as shopping, travel planning, and data management. Finding like-minded communities and audiences online is the goal; however, wherever you have people congregating, especially if there is potential for monetary gain, the risk of nefarious behavior rises. This has created an increased need for OSINT platforms [21].

The issue of comprehensive assistance to the military on thebattlefield, among other things, is ensured by the search and timely provision of information. OSINT, i.e. intelligence synthesized usingpublicly available data, is intended for this purpose. Digital traces left by users on open platforms are analyzed, which can help to find the geo-position of the enemy, its numbers, weapons, etc.

The following OSINT tools have become widely used: Offensive Security Cheatsheet, Osintia Social Media, FBI-tools by Daniel Durnea, Andy Black UK OSINT Toolkit, UK-OSINT. To understand the specifics of data collection from open sources, there are a number of special educational programs (courses and trainings): Arno Reuser's Trainings, IWS Training, Intel Techniques Online, Building an OSINT box, etc. [20].

The tools and programs covered will allow you to discover open ports and unsecured connected devices, install software, network device names and IP addresses, analyze data and software code, and more. The established disadvantages of OSINT tools are misuse of information and spending a lot of time on it.

2. Literature Analysis

OSINT is one from the forms of the process of organizing and managing the collection of intelligence data (Intelligence Collection Management), which includes their search and selection from publicly available sources, mining and analysis of information, formation of an intelligence document for making an appropriate decision. OSINT's

areas of interest include obtaining and analyzing official documents, draft statutes, tracking new scientific developments, databases, commercial and government websites, network diaries, and much more. Such a discipline complements the already existing ones, but does not become less important because of that [2].

OSINT is distinct from academic, business or journalistic research in that it represents the application of the proven process of national intelligence to a global diversity of sources, with the intent of producing tailored intelligence for the commander. OSINT is also unique, within a coalition operations context, in that it simultaneously provides a multi-lateral foundation for establishing a common view of the shared Area of Operations (AoO) [1]. An example of using OSINT as a universal data discovery tool is presented in Figure 1 [1].

Fig. 1. Relationship between Open Source and Classified Information Operations

OSINT is valuable to NATO member nations and to individual Partner nations in that it can be used to provide a common understanding of the AoO across all elements of its military forces and its civilian and non-governmental organization (NGO) counterparts. Elements of the forces not authorized access to the full range of classified information, often including such vital components, as military police, logistics elements, engineers, and the public affairs staff, can be made more effective through the utilization of tailored OSINT. At the same time, external parties with whom coordination is critical, but who are also not authorized access to classified information, can receive tailored OSINT that is helpful to a shared understanding of the AOO and the challenges facing the coalition and all its elements. Figure 2 illustrates this idea [1].

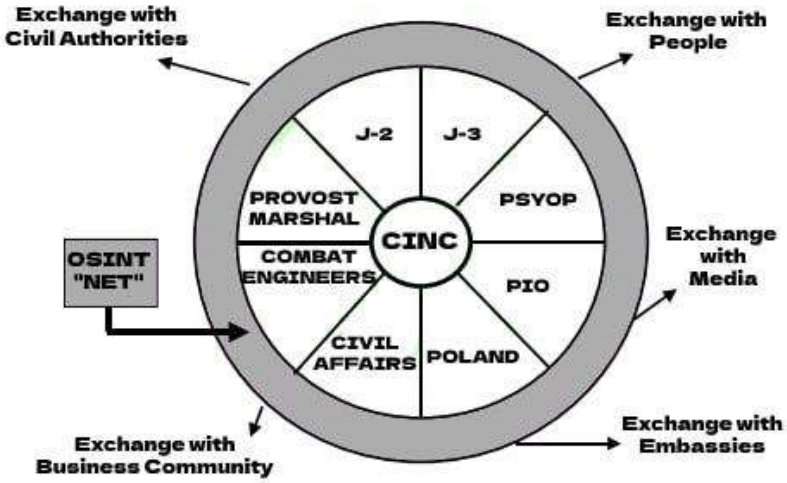

Fig. 2. Utility of OSINT Net for Internal and External Information Exchanges

OSINT is different from other forms of intelligence gathering in several ways, including the following:

1. OSINT is focused on publicly available and legally obtainable information, whereas other forms of intelligence gathering may involve confidential or classified sources.
2. OSINT uses various sources, including social media, news articles, public records, and government reports. In contrast, other forms of intelligence gathering may focus on a specific source type.
3. OSINT often involves using advanced analytical techniques, such as natural language processing and machine learning, to extract insights and intelligence from large volumes of data. In contrast, other forms of intelligence gathering may rely more on human analysis and interpretation [3].

The collection and analysis of OSINT information will be ultimately judged by its contribution to the overall intelligence effort. Collecting information from open sources is generally less expensive and less risky than collection from other intelligence sources. The use of OSINT may result not only in monetary savings but also in less risk than utilizing sensitive technical and human sources. OSINT can also provide insights into the types of developments that

may not be on the priority list for other systems or may not be susceptible to collection through other intelligence approaches – innovative applications of new technologies, shifts in popular attitudes, emergence of new political and religious movements, growing popular discontent, disillusionment with leadership [4]. By gathering publicly available sources of information about a particular target, an attacker – or friendly penetration tester – can profile a potential victim to better understand its characteristics and narrow the search area for possible vulnerabilities. Without actively engaging the target, the attacker can use the intelligence produced to build a threat model and develop a plan of attack. Targeted cyber attacks, like military attacks, begin with reconnaissance, and the first stage of digital reconnaissance is passively acquiring intelligence without alerting the target [3].

OSINT is an essential contextual and foundation element for classified intelligence operations. Overt human sources can help target and validate clandestine human intelligence (HUMINT) sources. Overt broadcast information can be used to better understand covertly collected signals intelligence (SIGINT). Commercial geospatial information, especially wide-area surveillance imagery, can be used to significantly enhance the value of the more narrowly focused covert imagery intelligence (IMINT) capabilities. OSINT can also make contributions to the emerging discipline of Measurements and Signatures Intelligence (MASINT), to Counterintelligence (CI), and to Operations Security (OPSEC). OSINT is the major new "force" in 21st Century Information Operations (IO) [1].

2.1. OSINT gathering techniques

Passive Collection - This is the most commonly used way to gather OSINT intelligence. It involves scraping publicly available websites, retrieving data from open APIs such as the Twitter API, or pulling data from deep web information sources. The data is then parsed and organized for consumption [5].

Active Collection - In this type, you interact directly with the system to gather intelligence about it, but The target can become aware of the reconnaissance process since the person/entity collecting information will use advanced techniques to harvest technical data about the target IT infrastructure such as accessing open ports, scanning vulnerabilities (unpatched Windows systems), scanning web server applications, and more. This traffic will look like suspicious behaviour and will more than likely leave traces on the target's intrusion detection system (IDS) or intrusion prevention system (IPS) [6].

From a technical view (Semi-passive), this type of gathering sends limited traffic to target servers to acquire general information about them. This traffic tries to resemble typical Internet traffic to avoid drawing any attention to your reconnaissance activities. In this way, you are not implementing in-depth investigation of the target's online resources, but only investigating lightly without launching any alarm on the target's side [7].

2.2. Main types and examples of OSINT data collection tools

FOCA is a tool that reads metadata from a wide range of formats documents and media. FOCA obtains the corresponding usernames, paths, software versions, printer details and email addresses mail All this can be done without the need for an individual download files. The metadata extraction process is almost completely automated. FOCA a domain is specified, and it is directed to search for all documents that exist in him FOCA is then notified that the documents need to be uploaded and extracted meta data It classifies each type it finds and displays them in a tree with convenient navigation. The metadata can then be exported to files so that you can was to manipulate them as in the example shown in Figure 3 [15].

Fig. 3. File search process using FOCA

Metagoofil – is an information gathering tool designed for extracting metadata of public documents (.pdf, .doc, .xls, .ppt, .docx, .pptx, .xlsx) belonging to a target company. Metagoofil will perform a search in Google to identify and download the documents to local disk. Figure 4 shows a list of available operations using Metagoofil. This one no longer extract the metadata [16].

```
root@kali:~# metagoofil -h
usage: metagoofil.py [-h] -d DOMAIN [-e DELAY] [-f] [-i URL_TIMEOUT]
                     [-l SEARCH_MAX] [-n DOWNLOAD_FILE_LIMIT]
                     [-o SAVE_DIRECTORY] [-r NUMBER_OF_THREADS] -t FILE_TYPES
                     [-u [USER_AGENT]] [-w]

Metagoofil - Search and download specific filetypes

options:
  -h, --help            show this help message and exit
  -d DOMAIN             Domain to search.
  -e DELAY              Delay (in seconds) between searches. If it's too small
                        Google may block your IP, too big and your searchmay
                        take a while. Default: 30.0
  -f                    Save the html links to html_links_<TIMESTAMP>.txt
                        file.
  -i URL_TIMEOUT        Number of seconds to wait before timeout for
                        unreachable/stale pages. Default: 15
  -l SEARCH_MAX         Maximum results to search. Default: 100
  -n DOWNLOAD_FILE_LIMIT
                        Maximum number of files to download per filetype.
                        Default: 100
  -o SAVE_DIRECTORY     Directory to save downloaded files. Default is current
                        working directory, "."
  -r NUMBER_OF_THREADS  Number of downloader threads. Default: 8
  -t FILE_TYPES         file_types to download
                        (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx). To search
                        all 17,576 three-letter file extensions, type "ALL"
  -u [USER_AGENT]       User-Agent for file retrieval against -d domain.
                        no -u = "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www
                        -u = Randomize User-Agent
                        -u "My custom user agent 2.0" = Your customized User-Agent
```

Активация Windows
Чтобы активировать Windows, пе
раздел "Параметры".

Fig. 4. Options of the Metagoofil

GeoSetter – is a freeware tool for Windows (requires Internet Explorer 10 or higher) for showing and changing geo data and other metadata (IPTC/XMP/Exif) of image files (e.g. images taken by digital cameras). Using GeoSetter you can do [16]:

- setting geo data by using embedded Google Maps map (requires internet connection) or by entering known values for coordinates and altitude directly;
- automatic filling of location IPTC fields and altitude values (requires internet connection);
- editable IPTC data (IPTC-NAA/XMP);
- possibility to change taken date of images;
- synchronization with track files (NMEA, GPX, PLT, Sony LOG, IGC and others);
- synchronization with already geo tagged images with buddy images (e.g.between RAW images and their corresponding JPEG images).

Wget - is a command line tool that can create HTTP, HTTPS and FTP connection to the site, mainly for automatic file extraction. It command line tool that is available for Linux, OSX and Windows. Wget you can instruct to view the links on the page and download all found image to a certain depth.

Shodan – is a search engine for Internet-connected devices. Web search engines, such as Google and Bing, are great for finding websites. Shodan gathers information about all devices directly connected to the Internet. If a device is directly hooked up to the Internet then Shodan queries it for various publicly-available information. The types of devices that are indexed can vary tremendously: ranging from small desktops up to nuclear power plants and everything in between. Figure 5 shows the result of a site scan using Shodan [17].

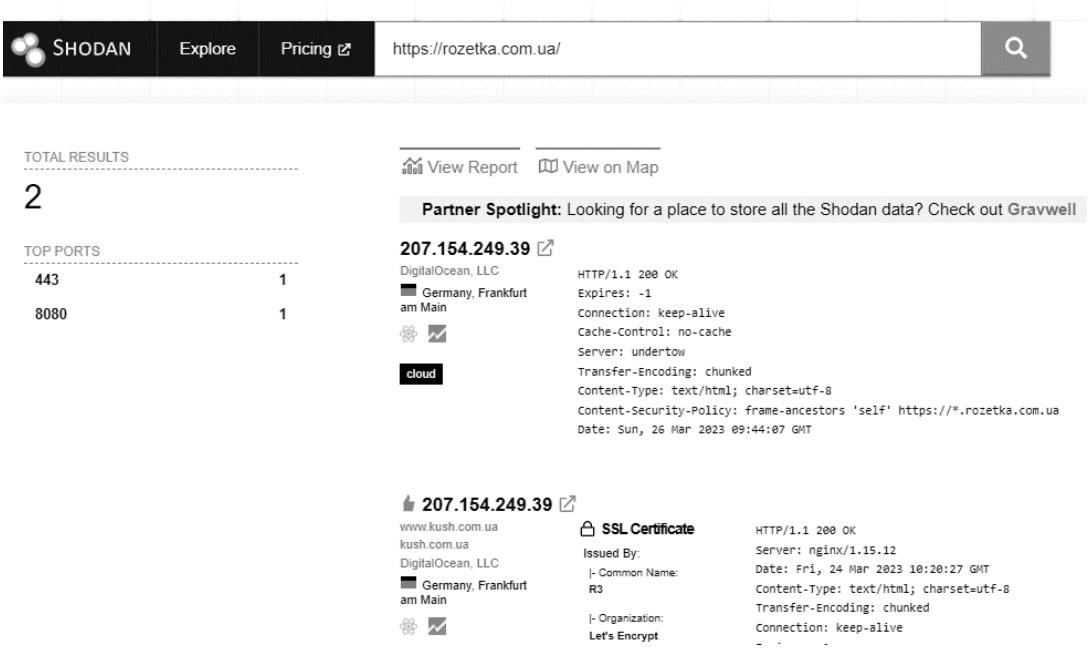

Fig. 5. Example using Shodan

2.3 OSINT skills

The four pillars to an OSINT strategy are sources, software, services and analysis. The private sector can address all four to some degree. Analysis is the key enabling skill that is essential to the successful integration of OSINT into an all-source intelligence product. Countermeasures against informational influences include, among other things, the formation of skills and abilities to work with information online, checkit, as well as used [18].

While some analysis of open sources can and should be acquired from private sources, those analytical skills necessary to integrate open source derived intelligence must be grown and nurtured within intelligence staffs. Analysis will be discussed further in Chapter III. This chapter is intended to expose the wider audience to the range of OSINT-related products that the private sector are optimized to provide [1].

Basic OSINT skills:

- work with search engines;
- google search engine;
- web data collection;
- reverse image search and research;
- research based on maps;
- content translation.

2.4 Classification of resources for OSINT operations

In the period from the Second World War to the present day, various terms have appeared to describe OSINT [8]:

- non-secret/ unclassified information – non-secret information;
- open/overt information – open information;
- overt intelligence – open intelligence;
- public information – publicly available public information;
- white intelligence – "white" intelligence.

Despite the highly specialized direction, the average reader or a person who is interested in this topic in view of the type of activity can use the document as a reference (guide) on the theory and practice of OSINT. The Doctrine states that the main difference between OSINT and other types of intelligence is that it is based on the source, information and methods of their collection, and not on a certain category of technical or human resources [10]. OSINT is intelligence that is carried out by collecting, processing and transmitting to the target addressee information from publicly available open sources for the purpose of solving specific intelligence tasks. OSINT is a significant area of intelligence activity that must be integrated into the intelligence cycle to ensure that decision makers and policymakers are fully informed. The distribution and use of verified information from open sources makes it possible to exchange such information, since hidden methods and secret sources are not used when obtaining it.

Open sources of information can be divided into 4 categories [9]:

- widely distributed data and information;
- targeted commercial data;
- expert assessments;
- "grey" literature.

Also, to open sources and publicly available information include [10, 14, 15]:

- diplomatic missions (Diplomatic Missions);
- Chambers of Commerce;
- non-governmental organizations (Non-Governmental Organizations);
- religious organizations (Religious Organizations);
- national-level intelligence organizations (National-Level Intelligence Organizations);
- the academic field – software, dissertations, lectures, presentations, research works, knowledge in printed and electronic form on economics, geography (physical, cultural, military-political), international relations, regional security, science and technology;
- state, intergovernmental and non-governmental organizations – databases, published information, and printed reports, wide-ranging reviews in the economy, environment, geography, humanities, security, science and technology;
- commercial and public information services – disseminated, published, printed news of current international, regional and local events;
- archives (libraries) and research centers – printed documents and digital databases on a number of issues such as knowledge and skills of information search;
- individual and group information – handwritten, drawn, published, printed or distributed information (eg art, graffiti, flyers, posters or websites);

The NATO OSINT Reader focuses on the "grey literature" category. It can include scientific reports, technical manuals, economic reports, working papers, non-official government documents, dissertations, marketing studies, newsletters and much more. All these materials cover the scientific, political, socio-economic and military spheres [11]. In terms of intelligence terminology, OSINT is information relevant to intelligence requirements obtained through the systematic collection, processing and analysis of publicly available information. This term includes two complementary components [12]:

- open source – information provided by a person or group without expectations of confidentiality;
- publicly available information – data, facts, instructions or other materials published or transmitted to the general public, available upon request by any person, lawfully seen or heard by any casual observer or disclosed at meetings open to the general public.

The NATO OSINT Handbook also uses the concept of Open Source Data (OSD), which consists in collecting raw data from many different sources – it is therefore a stage of aggregating information without analyzing and processing this data [13].

Open sources and publicly available information may include, but are not limited to, the following types [12]:

- academic field – software, dissertations, lectures, presentations, research works, knowledge in printed and electronic form on economics, geography (physical, cultural, military-political), international relations, regional security, science and technology;
- governmental, intergovernmental and non-governmental organizations (NGOs) – databases, published information, and printed reports, reviews of a wide range in the economy, environment, geography, humanitarian sciences, security, science and technology;
- commercial and public information services – disseminated, published, printed news of current international, regional and local events;
- archives (libraries) and research centers – printed documents and digital databases on a number of issues such as knowledge and skills of information search;
- individual and group (information) – handwritten, drawn, published, printed or disseminated information (for example, art, graffiti, leaflets, posters or websites in three main stages of OSINT work: information gathering, data cleaning and analysis of "clean" data. Also, the goal is to verify the authenticity of the information provided based on metadata or analysis of geolocation data.

The problem being addressed is the development of an algorithm for the effective and efficient use of Open-Source Intelligence (OSINT) technology in modern services. The goal is to create a step-by-step process that can be used by organizations to collect, analyze, and utilize publicly available information to improve their operations, enhance threat detection and response, and gain competitive advantages. The algorithm must take into account the potential risks and limitations associated with OSINT technology, such as accuracy, privacy, and data protection concerns, and provide appropriate safeguards and controls to ensure that the information gathered and analyzed is reliable and secure.

3. Methods And Materials Of Research

Object of research: mechanisms of obtaining information from open sources using OSINT and means of monitoring the activity of research objects.

Subject of research: finding and obtaining information from open sources using OSINT.

Research methods: theoretical – method of formalization, method of analogy, comparison of various tools and techniques of OSINT application, design and modeling for processing the results of the experiment; empirical methods – observation and research of specific phenomena, experiment, as well as generalization, classification and description of the results of research and experiment, their implementation in the practical activities of people; experimental method was used on the basis of which the general scheme (algorithm) of using OSINT tools for finding the information using

modern social networks was derived. An example of the application of the empirical method is shown in figure 6.

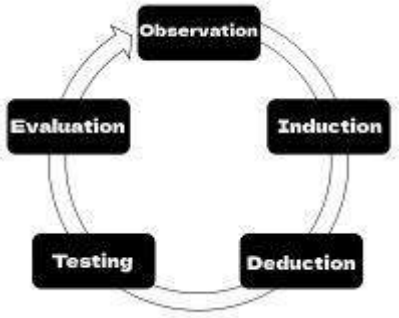

Fig. 6. Empirical methods (as the basis of the OSINT usage example)

4. Results

The developed OSINT block diagram (algorithm) is intended primarily for the study of objects that use social networks and modern services (including entertainment ones) (actively or simply registered an account). The purpose of this scheme is to collect data (from active/very active users of information collection on an ongoing basis) primarily about a group of people based on modern services (TikTok, YouTube Shorts) using publicly available OSINT tools for data analysis, collection and processing (or data arrays).

The basis of data collection is the low cyber hygiene of the research objects (users), careless attitude to the distribution of their own confidential data (including the creation of accounts in social networks with the indication of personal data; direct inclusion in TikTok, YouTube Shorts, which can reveal the location of the object; posts and comments that can provide data on the circle of communication of the object under study, his friends, relatives, place of work, etc).

In this algorithm, special attention is paid to the issue of security and elements of its provision of publicly available applications and tools (preserving security and confidentiality allows to maximize the time during which it is possible to observe and collect data about the object and ensure the integrity and availability of the received information when it is transmitted through secure communication channels). The peculiarity of using TikTok and YouTube Shorts for OSINT operations is that after correctly configuring the recommendations, these services themselves will begin to "help" you by providing information about the social circle of the subject being investigated, his preferences, whereabouts, personal data indicated by the person in the video, which can help with detailed study of the object. By collecting information from short video materials, you can learn a lot of confidential information that will be revealed without even guessing about its value and the possibility of using it about the same person.

When using this scheme, specialists are recommended to have minimal knowledge of recommendation algorithms in social networks and other skills described in point 2.3 "OSINT skills".

Figure 7 shows the working algorithm for finding information from open sources using OSINT technology. This algorithm allows you to reduce the time of information collection and increase the reliability and completeness of the data obtained.

To implement the proposed algorithm is advisable to perform the next sequence of actions:

Step 1: determination of the main objective of the OSINT operation (how many people will be investigated, what information should be obtained, what tools should be used). Analysis of the tools that will be used for each individual case (Shodan, Google Docker, Metagoofil, Whois, etc.)

Step 2: choosing a place of work to conduct an OSINT operation (cafe, office, park, etc.). Provision of a secure Internet connection (recommended) or connection to public networks. Using the tools from Step 1, we find the minimum data (first of all, the name of the country and full name) and the browser anti-detection (recommended use in combination: TOR browser + proxy server with the IP address of the country of the research object)

Step 3: we choose a mobile emulator (be sure to choose the same country as the object under study in case of successful data acquisition) while connecting a VPN (recommended) with the same country as the object under study.

Step 4: combine the tools used in Step 2 and Step 3 into a virtual machine. We create an account in the required social network (service): we use the same data (region, phone number of the country, personal preferences) as that of the object under study (this will help us to optimize the recommendations in the next steps to obtain maximum informativeness) to preserve confidentiality.

Step 5: we detail the received information about the object as much as possible (recommended) and apply it when setting up recommendations: setting tags, activity in comments, likes for videos, subscriptions to other accounts that have at least some relation to our object. If necessary, we automate this process using artificial intelligence algorithms or adjust recommendations manually.

Step 6: collection of data obtained as a result of observations after setting recommendations (primarily TikTok and YouTube).

Step 7: if necessary, we determine the geoposition of the object based on the received data array (we use GEOINT).

Step 8: we detail the personal data obtained in the course of OSINT intelligence, using OSINT tools (examples of programs are mentioned in point 2.2). We sort the received data by importance and value for final report.

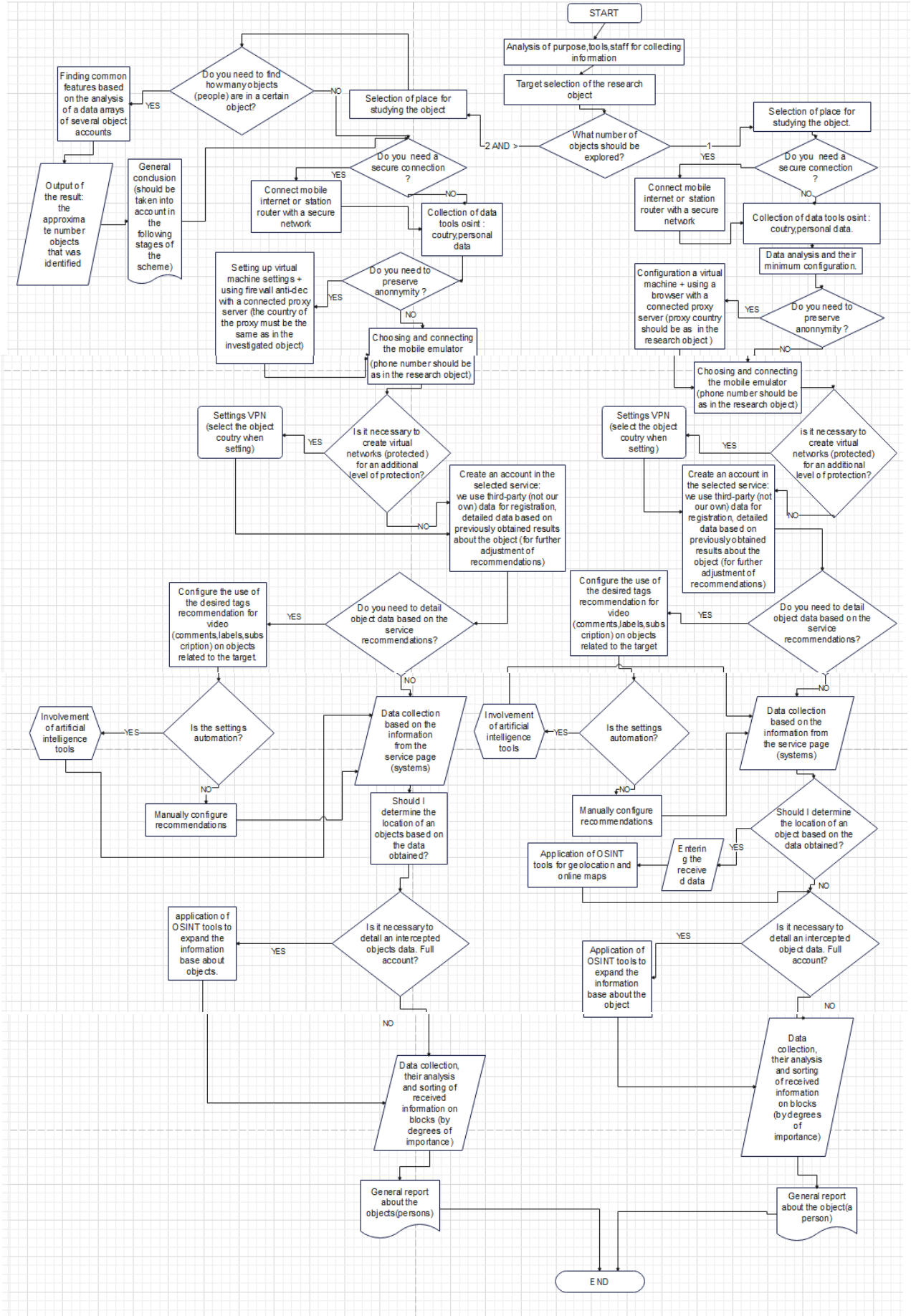

Fig. 7. The resulting algorithm for searching information in modern services.

Discussion Of Results

The algorithm of using the OSINT technology in modern services has been developed. The proposed algorithm for using OSINT technology in modern services allows you to obtain the maximum amount of data, minimize resources and time, and takes into account the peculiarities of the legislation of the country of the OSINT object. One of the key benefits of using OSINT technology in modern services is that it allows organizations to gather information quickly and efficiently. By leveraging automated tools and algorithms, it is possible to collect vast amounts of data from a wide range of sources, including social media, news sites, and government databases. This information can then be analyzed to identify patterns, trends, and potential risks. Another benefit of using OSINT technology is that it can help organizations to identify and respond to potential threats more quickly. This algorithm can allow organizations to take proactive measures to mitigate the risk of these threats. However, there are also some potential risks and limitations associated with the use of OSINT technology in modern services. For example, there is a risk that the information gathered may be inaccurate or incomplete, which could lead to incorrect conclusions or decisions. Additionally, there are concerns around privacy and data protection, particularly in relation to the collection and use of personal data. In conclusion, the use of OSINT technology in modern services has the potential to provide significant benefits to organizations, including faster and more efficient information gathering, and improved threat detection and response.

5. Conclusions

Many processes take place on the Internet, and modern security strategies must be based on the masses of social data that are created every day. Collecting, filtering and analyzing this information requires enhanced capabilities of OSINT platforms.

In the course of research, a general scheme and algorithm of data collection by OSINT methods using modern services (TikTok, YouTube Shorts, etc.) along with other OSINT tools for collecting, processing and analyzing information on a temporary or permanent basis was proposed.

For the successful conduct of OSINT operations, special attention must be paid to the personal skills and abilities of the OSINT specialist high: theoretical (knowledge of regulatory and legal support and legislation of the country in which OSINT operations will be conducted, schemes and algorithms of OSINT intelligence stages) and practical (ability to use modern OSINT tools, search for various information in a protected mode using the Internet, etc.) knowledge and skills of specialists in the field of OSINT.

Not only can OSINT help protect against covert, deliberate attacks such as information leakage, theft, and fraud, but it also has the ability to gain real-time and location-based situational awareness to help protect people at work, at events, in facilities, or even in retail. center. The right OSINT toolkit will give security and intelligence teams an edge.

The proposed algorithm allows to reduce the time to collect information and increase the reliability and completeness of the obtained data. The set goal has been achieved.

References

[1]. NATO Open Source Intelligence Handbook [Electronic resource]. – Access mode:https://web.archive.org/web/20201107103435/http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20%20Jan%202002.pdf (in Eng.)

[2]. Kozhushko O.O. (2011) .*OPEN SOURCE INTELLIGENCE (OSINT) IN INTELLIGENCE US PRACTICES*. https://ena.lpnu.ua:8443/server/api/core/bitstreams/a964dfbb-a16d-4e8a-b621-9aa6cb277197/content (in Ukr.)

[3]. Sentinel One company. What.(2019, June 17).*Is Open Source Intelligence (OSINT).* https://www.sentinelone.com/cybersecurity-101/open-source-intelligence-osint/ (in Eng.)

[4]. Richard A., Best Jr., Cumming A..*Open Source Intelligence (OSINT): Issues for Congress*.CRS: report for Congress. https://sgp.fas.org/crs/intel/RL34270.pdf (in Eng.)

[5]. Imperva company.(2022, September 20). *Open-Source Intelligence (OSINT)*. https://www.imperva.com/learn/application-security/open-source-intelligence-osint/ (in Eng.)

[6]. Guise Bule.(2020). *A Guide To Open Source Intelligence (OSINT)*.https://itsec.group/blog-post-osint-guide-part-1.html (in Eng.)

[7]. Nihad Hassan.(2018, August 12). *An Introduction To Open Source Intelligence (OSINT) Gathering*. https://www.secjuice.com/introduction-to-open-source-intelligence-osint/ (in Eng.)

[8]. Hamilton, B. The DNI's Open Source Center: An Organizational Communication Perspective / B. Hamilton // International Journal of Intelligence and CounterIntelligence [Electronic resource]. – Access mode: http://www.oss.net/dynamaster/file_archive/110802/98532478899216432d3d76e2f9d4534c/20110802%20Dr.%20Bean%20IJIC%20Open%20Source%20Center.pdf (in Eng.)

[9]. Electronic encyclopedia Wikipedia. [Electronic resource]. – Access mode: http://en.wikipedia.org/wiki/Foreign_Broadcast_Information_Service (in Eng.)

[10]. Open Source Intelligence, U.S. Army Field Manual Interim FMI 2-22.9, December 2006 [Electronic resource]. – Access mode: www.fas.org/irp/ doddir/ army/ fmi2-22-9.pdf (in Eng.)

[11]. Electronic encyclopedia Wikipedia. [Electronic resource]. – Access mode: http://en.wikipedia.org/wiki/Director_of_National_Intelligence(in Eng.)

[12]. Electronic encyclopedia Wikipedia. [Electronic resource]. – Access mode: http://en.wikipedia.org/wiki/United_States_Intelligence_Community (in Eng.)
[13]. Transparent Data (Oct 16, 2020). *OSINT – What is it and what does it have to do with open sources of information?* https://medium.com/transparent-data-eng/osint-what-is-it-and-what-does-it-have-to-do-with-open-sources-of-information-ec35daeea1c0
[14]. Blackdot Solutions.*OSINT Sources: What Are The Different Types of Open Source Data?*. https://blackdotsolutions.com/blog/osint-sources/ (in Eng.)
[15]. NATO Open Source Intelligence Reader, February 2002 [Electronic resource]. – Access mode: https://web.archive.org/web/20060104082427/http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf (in Eng.)
[16].Christian Martorella (2022, August 05). *metagoofil Usage Example* https://www.ali.org/tools/metagoofil/ (in Eng.)
[17].Friedemann Schmidt.*GEOSETTER DESCRIPTION*. https://geosetter.de/en/main-en/ (in Eng.)
[18]. John Matherly *What is Shodan?*. https://help.shodan.io/the-basics/what-is-shodan (in Eng.)
[19].Ufimtseva O.S. . *USING OSINT IN THE CONDITIONS OF ARMED AGGRESSION OF THE RUSSIA AGAINST UKRAINE. [Scientific thesis, SSU Academy]* http://dspace.onua.edu.ua/bitstream/handle/11300/19841/%D0%A3%D1%84%D1%96%D0%BC%D1%86%D0%B5%D0%B2%D0%B0%20%D0%9E%D0%BB%D0%B5%D0%BD%D0%B0%20%D0%A1%D0%B5%D1%80%D0%B3%D1%96%D1%97%D0%B2%D0%BD%D0%B0.pdf?sequence=1&isAllowed=y (in Ukr.)
[20].Victor Borisov.*OSINT tools*.https://start.me/p/Om8DeX/osint-tools (in Eng.)
[21]. Flashpoint Team.(August 2, 2022). *What Is Open Source Intelligence: The Importance of OSINT in Your Organization's Threat Landscape*.https://flashpoint.io/blog/what-is-osint-open-source-intelligence (in Eng.)

Отримана в редакції 01.02.2023. Прийнята до друку 03.03.2023. Received 01 February 2023. Approved 14 March 2023. Available in Internet 12 April 2023.