Methods of information systems synthesis

UDC 004.032.26, 528.854 **doi:** https://doi.org/10.20998/2522-9052.2024.1.04

Serhii Herasymov[1], Andrii Tkachov[1], Sergii Bazarnyi[2]

[1] National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine
[2] The National Defense University of Ukraine, Kyiv, Ukraine

COMPLEX METHOD OF DETERMINING THE LOCATION OF SOCIAL NETWORK AGENTS IN THE INTERESTS OF INFORMATION OPERATIONS

Abstract. The researcher **developed a method** for determining the location of social network agents in the interest of conducting an information operation based on a comprehensive approach to data analysis of the information system. **The relevance of the method** is determined by the need to specify the enemy's target audience in the area of the information operation. **Results.** The author proposed a complex method for determining the location of social network agents, which is based on the combination of data from the analysis of the social connections of the specified agent, geotags and the time of registration of his friends in the social network, databases of IP addresses and geolocations of social network agents. The advantage of the developed method is the possibility of its application without direct access to the devices of agents of the social network that use the data of global positioning satellite systems. **Conclusion.** The application of the proposed complex method of determining the location of agents of social networks makes it possible to increase the effectiveness of information operations due to a more accurate definition of the enemy's target audience in the area of operations. The direction of improvement of the developed method can be its integration with complex information systems of psychological influence, as well as the use of machine learning methods and algorithms.

Keywords: social network agent; geolocation; geotag, information system; target audience; psychological influence.

Introduction

Today in the world there is a significant increase in armed aggression between states in different parts of the world. However, a feature of the modern armed struggle is the widespread use of information operations, which are aimed at internal and external target audiences (TA) with the task of justifying their aggressive actions and convincing their own population and the public of other countries of the legitimacy of the resolution of the armed conflict (aggression). According to research by specialists in the field of information and psychological operations, the essence of information operations is defined as "the ability, in combination with other means, to conduct massive information campaigns against the population of states to destabilize society and the government, forcing the state to make decisions in the interests of the opposite party" [1].

Information operations and psychological operations are conducted in order to counter the enemy's information operations, to create favorable conditions for the use of their troops (forces) and to prepare the population to fight the enemy. Such operations also include psychological actions and distribution of prepared special information (SI) for psychological influence) on the emotions, motives, rational thinking and behavior of the enemy's target audience.

Information operations involve the implementation of planned actions with the delivery of specially prepared information using means of communication to influence the emotions, motives, rational thinking and behavior of the target audience in order to achieve political and military goals [2]. Possible means of disseminating information during the information operations can be: sending short messages (SMS) to mobile phones in a certain area, radio appeals, sound broadcasting stations, printed products (postcards, newspapers), etc. In modern conditions, the greatest attention is paid to the means of information dissemination on the Internet, especially in social networks (SN).

A key condition for achieving the goals in the implementation of the information operations is the correct definition of the target audiences – groups of people selected for the implementation of psychological influence by the forces and means of the information operations [2].

One of the main factors that significantly affects the effectiveness of the information operations is the correct definition of the target audiences, for which it is necessary to have information about the geographic location of specific persons or groups of persons who are selected for the implementation of psychological influence.

It is also necessary to take into account the potential level of psychological influence of social networks agents, which have the greatest influence on the determined targets audiences according to the method based on the calculation of the level of publishing activity and the number of network connections of agents in social networks [3].

Object, subject and methods of research. Determining the geographic location of social networks agents or the geolocation of social networks agents is an important task that must be solved when determining the target audiences for the further development of special information products (informational materials for the implementation of psychological influence).

Determining the actual stay in the area of the information operations of the social networks agents is an important task due to the reluctance of the social networks agents to disclose personal information about their location.

Thus, the key condition for achieving the goals of conducting psychological influence is the correct definition of target audiences, which will increase the effectiveness of conducting psychological influence.

Literature analysis. The geographic location (geolocation) of social networks agents who have not specified their own location in the profile can be determined using various methods. Methods for determining the location of social networks agents based on the selection and subsequent analysis of keywords (indicators) in the text of messages published by social networks agents are described in [4]. These methods use different methods of finding relevant words and their correlation with the geolocation of the social network's agent.

To increase the accuracy of geolocation determination based on content analysis created by social networks agents, methods built on the basis of neural networks are used [5].

Another group of methods is used to specify the geolocation of social networks agents by analyzing network connections between agents using a graph model of social networks [6, 7].

These methods take into account the analysis of the interaction of social networks agents, their connections with each other (one-way or two-way), the degree of proximity in the network using various methods of learning graphs.

The study of the types of connections between social networks agents and the analysis of their content - reviews of the same places on Google maps are given in work [8].

Based on the analysis of the profile data of social networks agents and their metadata (for example, the time zone, the country in the profile, and other indicators), the probability of determining the location of the social network's agent, which was investigated in [9, 10], increases.

In [11], IP address geolocation studies were conducted using active signal delay measurements (GeoPing), DNS routing determination (GeoTrack), and the use of IP databases of commercial services (for example, IP2Location and MaxMind) for geolocation.

Presentation of the main research material

Most of the gadgets used by social networks agents have the function of determining their own location using satellite navigation technologies (GPS) or using the triangulation method based on the reception and transmission stations of the mobile operator's network (A-location). Therefore, the content created by social networks agents (text messages, photos, video materials) may have markers that indicate the geographical location of the social networks agent at the time of creation (distribution or posting) of the corresponding content, even if he, the social networks agent, did not indicate his own location in the social networks own profile.

According to statistical data presented in work [12], it was determined that the majority of mobile phone (gadget) users do not prohibit the use of geolocation in the settings for the full operation of applications and services that work on the basis of data about the location of the mobile gadget (for example, rational routes on maps Google, availability of necessary shops nearby, etc.). If in the device settings, the social networks agent has given permission to store the history of the location of the device, then the movement history of the social network's agent with the gadget (mobile phone) can be obtained by applications that have been granted access to geodata. Later, the social networks agent can view the places it visited and adjust the geodata. Applications that have access to geodata can determine the location of the gadget (by mobile phone number or code) to display relevant information (services, advertising, etc.) to the social network's agent.

In the settings of the gadget (mobile phone), the social networks agent can independently prohibit the use of the Global Positioning System (GPS) of the GPS location, but leave the possibility of using the A-location, then the accuracy of the geolocation decreases. The use of A-location technology provides an opportunity to connect the nearest base stations and their geographic coordinates with the gadget of the social network's agent at the current moment in time. The use of A-location technology provides such opportunities as:

location determination without the need to install additional software on the social networks agent's gadget, using the existing mobile communication infrastructure;

does not require the consent or informing of the social networks agent about determining his location;

can be used in rooms and other locations where there is no GPS satellite navigation signal.

Therefore, A-location technology is a potentially effective tool for solving the problem of determining the geographic location of social networks agents, which should be combined with other approaches and methods to increase the overall accuracy of geolocation. But at the same time, the question arises as to how to solve the problem of determining the geolocation of those social networks agents who hide information about their own location for reasons of confidentiality or for other reasons and have prohibited the use of GPS location and A-location in the phone settings.

To increase the accuracy of geolocation, the social networks agent can allow the device to determine the location automatically based on the Wi-Fi access point information [13, 14]. Some applications may automatically send anonymized device geolocation statistics (for example, to Google).

During emergency calls, geodata about the location of the social network's agent is automatically sent from the gadget directly to emergency services without the permission of the social network's agent. However, the study [12] provides statistics that reflect the information that among the published materials, only 10% of the content has geographical tags.

Using methods of cyber influence, information about the location of the social network's agent can be obtained, but this is beyond the scope of scientific research.

The assumption of the developed method is that the social networks agent has only one permanent geographical location (latitude and longitude), where he is constantly is located and has access to the Internet (as

a rule, this can be a place of residence or a place of work). Each social networks agent has connections with other social networks agents, some of whom are his friends and with whom he is systematically in the same place (for example, the social networks agents A and B), as evidenced by the history of registrations on Google Maps likes and comments they leave after visiting the places marked on the maps (Fig. 1).

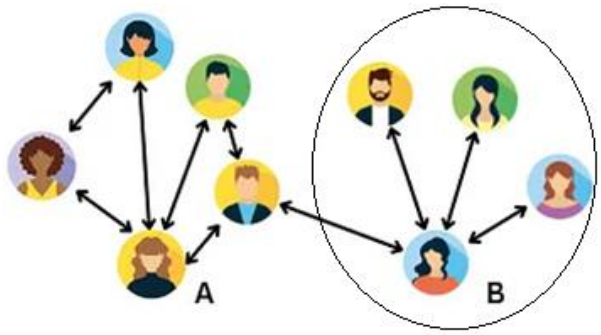

Fig. 1. Example of social connections of social network agents

In most cases, the location of the social network's agent is correlated with the location (registration locations) of his friends. An example of such social ties to agent *B* is circled in Fig. 1.

The reliable determination of the location of the social networks agents provides an opportunity to increase the effectiveness of the information operations due to the accurate determination of the target audiences that is subject to psychological influence. For further psychological influence, it is expedient to specify target audiences – friends of the social networks agent who live with him in the same settlement.

In [15], the scientific and applied problem of detecting spammers and identifying spam messages in the text context of any social network or messenger was solved. Such a task is solved using various spam detection algorithms and spammer detection approaches. The results of the study [15] allow the social networks agent to detect and filter out real and virtual (spammers), but do not allow determining its location.

In most cases, the social networks agent has two areas of concentration of points on the registration map (Google Maps) – near the place of work during the day and the place of rest at night, which are on average up to 15 km away for a resident of a large city. To determine the target audiences in the interests of the information operations, it is enough to have information about the location of the social network's agents with accuracy to the population center. The technology for determining the location of the device by its IP address (which is provided by the Internet provider for a stationary connection) has such accuracy, and on average it is (10...30) km depending on the network infrastructure [14].

In [14], geolocation research was carried out using databases of IP addresses, access to which is free (IP2Location and MaxMind). Special IP address databases of the social networks agents identify the geographic region, city, and country associated with the IP addresses.

The accuracy of determining the location of the social networks agents using IP geolocation databases was studied in [16].

Commercial versions of these databases have a larger number of addresses and provide a more complete set of services. In [16] it was determined that the error of determining the location for fixed networks of Internet providers is up to 5 km on average, and for networks of mobile operators up to 10 km.

But in order to determine the location of social networks agents using IP geolocation databases, it is necessary to additionally have information about the IP of social networks agents.

It is important to note that most social networks set restrictions on access to information about IP addresses of social networks agents.

The task of determining IP addresses of social networks users can be solved using social engineering methods.

In [17], two-factor authentication is used, when the authorization code is sent through a separate channel. This approach, admittedly, is associated with significant overhead costs associated with both the use of additional channels and the need for additional processing. At the same time, there is no analysis of the impact of costs on improving security and availability during information transmission. Apart from research, there is also the determination of the geographical location of information channels.

In work [18], the security of information transmission is considered physically as an additional level of security that ensures the confidentiality of radio communication.

The typical characteristics of a wireless channel (noise, interference) can be used to preserve the confidentiality of a message from potential interceptors. Coordinated planning of the inclusion of channels between different cells using the same radio resources is proposed, based on the use of spatial information in the form of an IP address [19, 20].

We do not consider the method of determining the IP addresses of the social networks agents by means of cyber influence with the help of unauthorized access to the databases of the provider's website, which provides customers with access to the Internet, due to the violation of legal norms.

There is a way to determine the IP addresses of the social networks agents by the "phishing" method [21] (by sending personal messages to specified the social networks agents with a request to respond through their e-mail), which consists of the following:

– we send a useful offer to a designated the social networks agent, whom we will designate *as B*, a personal message through the social networks;

– we invite him to reply to the e-mail address you specified;

– if agent *B* sent a reply letter with his e-mail address, the next step is to perform service data analysis of the received letter, which is carried out using "online" or "offline" mail programs. Using the specified service, the IP address of agent *B can be found* in the "mail properties" section of the mail server.

The second way to determine the IP address of the social networks agent is to encourage it to go to an interesting link, an image, which results in an automatic redirection to a service for determining IP addresses, for example – IP Logger [22, 23].

To generate a link on the IP Logger site, in the "link/picture" block, you need to put the link of the specified the social networks and click "get logger code".

The next step is to store the ID-own logger in the system for statistics analysis.

After performing the above actions, send agent *B* a message with the link "Your link for collecting IP addresses" and invite him to follow this link. In order to distract agent *B,* it is necessary to create a short link using Google tools.

After agent *B* follows the link we specified, he will go to the page whose address was specified on the IP Logger's main page, and his IP address will be displayed in the statistics on the ID page of this logger.

To increase the probability of correctly determining the location of a social networks agent, it is most appropriate to develop a comprehensive method that combines the method of determining the location of the social networks agents by analyzing IP geolocation databases and specifying the location of the social networks agents by analyzing their geotags.

The developed method consists of the following stages.

1. Finding the set of friends of a specified the social networks agent (B_u; t_u).

2. Finding the IP of each friend of the social network's agent from a defined set of his friends.

3. Based on the found IPs, using IP geolocation databases, the target audiences are determined, which includes those friends of the social networks agent who live in the same city.

4. In order to exclude the influence of errors in the IP geolocation databases, the registration places of the friends of the social networks agent are checked (by place and time: B_{fn}; t_{fn}), which determines their most likely permanent location

5. According to the result of the target audience's refinement by the method of excluding from the target audiences those social networks agents, most of whose registrations are in other places, the final target audiences are formed based on the same geographical location of the social networks agents.

Schematically, a complex method of determining the location of the social networks agents based on the analysis of their geotags, taking into account the information of geolocation databases by IP, is shown in Fig. 2.

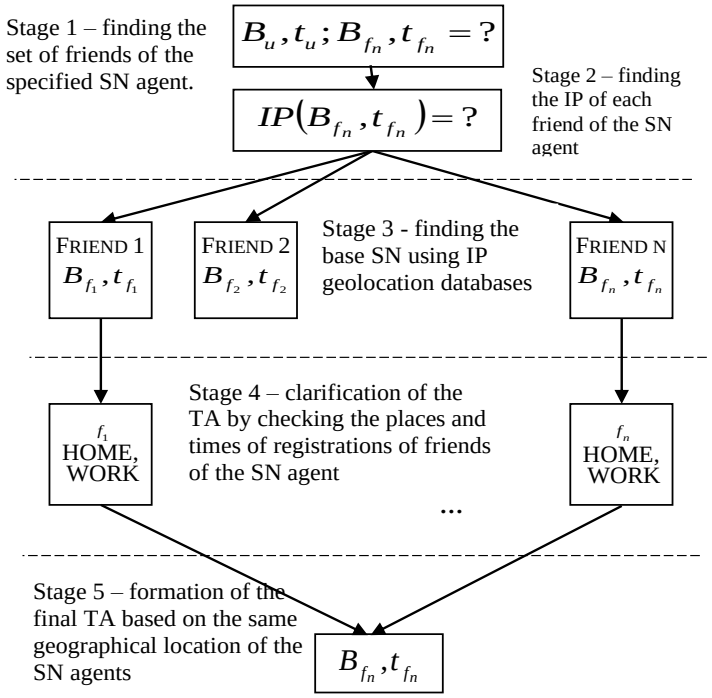

Fig. 2. A comprehensive method of determining the location of the social networks agents by analyzing their geotags, taking into account the information of geolocation databases by IP

Let's consider additional existing tools, namely:

WHOIS is a web service that verifies information about the owner of a domain or IP address. Entering an IP address or domain into the WHOIS interface allows you to get information about the owner, contact details and location.

The IP info service is used to obtain information about the geographical location of an IP address.

Web application firewalls (WAFs) record information about the IP addresses from which HTTP requests are received and contain the functionality of their analysis.

With the help of specialized tools for analyzing network activity Wireshark, Snort, or Bro, it is possible to analyze network traffic and determine the IP addresses of the social network's agents [24, 25].

In order to detect the social networks agents that use VPN anonymizers or proxy servers to hide their IP address, you can use the software module for determining the use of VPN/Proxy by the social networks agents, as a component of the software and technical complex of network data processing, described in [26, 27]. Using the above tools for monitoring network activity and detecting IP addresses of the social network's agents, the following tasks can be additionally solved:

– first, to determine the behavior of the social network's agents, the spread of fake news or propaganda. The analysis of the IP address provides information about the geographical location of the social network's agents, which is necessary for conducting information operations and cyber-attacks;

– secondly, to detect bots, block the spread of malicious content, and protect against DDoS attacks. The social networks administration can also independently use IP addresses for content moderation.

Conclusions

Thus, the first comprehensive method of determining the location of the social networks agents has been developed based on the integration of IP address geolocation databases and the analysis of geotags of the social networks agents, which makes it possible to increase the reliability of determining the target audiences by geographical location in the interests of conducting information operations.

The direction of further research may be the development of methods for determining target audiences based on other approaches, such as the analysis of network connections of the social network's agents, or the analysis of additional information from the content of profiles of the social network's agents. It is also promising to develop automation tools using machine learning to implement the stages of the developed method.

REFERENCES

1. Yevseyev, S., Ponomarenko, V., Laptiev, O. et. al. (2021), *Synergy of building cybersecurity systems*, RS TECHNOLOGY CENTER, Kharkiv, 188 p., doi: https://doi: 10.15587/978-617-7319-31-2
2. (2014), *AJP-3.10.1. Allied Joint Doctrine for Psychological Operations*, Edition B, Version 1, NATO doctrine, September 2014, 106 p., available at: https://info.publicintelligence.net/NATO-PSYOPS.pdf
3. Bazarnyi, S. V. (2023), "A method of identifying agents of social networks with the greatest influence", *Modern information technologies in the field of security and defense: science*, No. 1(46)/2023, pp. 145–150, doi: https://doi.org/10.33099/2311-7249/2023-46-1-145-150.
4. Mourad, A., Scholer, F., Sanderson, M. and Magdy, W. (2018), "How well did you locate me?: effective evaluation of Twitter user geolocation", *ASONAM '18: Proceedings of the 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, August 2018, pp. 437–440, available at: https://dl.acm.org/doi/10.5555/3382225.3382317
5. Zhong, T., Wang, T., Wang, J., Wu, J. and Zhou, F. (2020), "Multiple-aspect Attentional Graph Neural Networks for Online Social Network User Localization", *IEEE Access* (IF3.367), Vol. 8, pp. 95223–95234, doi: https://doi.org/10.1109/ACCESS.2020.2993876
6. McCallum, A., Nigam, K. (1998), "A Comparison of Event Models for Naive Bayes Text Classification," *AAAI 1998: Learning for Text Categorization*, pp. 41–48, available at: http://courses.washington.edu/ling572/papers/mccallum1998_AAAI.pdf
7. Zhang, W. and Gao, F. (2013), "Performance analysis and improvement of naïve Bayes in text classification application", *Proceedings of the IEEE Conference Anthology*, China, pp. 1–4. doi: https://doi.org/10.1109/ANTHOLOGY.2013.6784818
8. Rahimi, A., Cohn, T. and Baldwin, T. (2017), "A Neural Model for User Geolocation and Lexical Dialectology", *Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics*, Association for Computational Linguistics Vancouver, Canada, Vol. 2, Short Papers, pp. 209–216, available at: https://aclanthology.org/P17-2033.pdf
9. Zola, P., Cortez, P. and Carpita, M. (2019), "Twitter user geolocation using web country noun searches," *Decision Support Systems*, Vol. 120, pp. 50–59, doi: https://doi.org/10.1016/j.dss.2019.03.006
10. Semenov, S., Sira, O., Gavrylenko, S. and Kuchuk, N. (2019), "Identification of the state of an object under conditions of fuzzy input data", Eastern-European Journal of Enterprise Technologies, Vol 1, No 4 (97), pp. 22-30, doi: https://doi.org/10.15587/1729-4061.2019.157085
11. Dan, O., Parikh, V. and Davison, B. (2018), "IP Geolocation through Reverse DNS", *Networking and Internet Architecture*, abs/1811.04288 (2018), pp. 1–10, doi: https://doi.org/10.48550/arXiv.1811.04288
12. Kong, L., Liu, Z. and Huang, Y. (2014), "Spot: Locating social media users based on social network context". *Proceedings of the VLDB Endowment*, vol. 7, no. 13, pp. 1681–1684, doi: https://doi.org/10.14778/2733004.2733060
13. Kuchuk, N., Mozhaiev, O., Semenov, S., Haichenko, A., Kuchuk, H., Tiulieniev, S., Mozhaiev, M., Davydov, V., Brusakova, O. and Gnusov, Y. (2023), "Devising a method for balancing the load on a territorially distributed foggy environment", *Eastern-European Journal of Enterprise Technologies*, Vol. 1(4-121), pp. 48–55, doi: http://dx.doi.org/10.15587/1729-4061.2023.274177
14. Sandeep, Singhal (2002), "Top 10 vulnerabilities in Today`s WI-FI Networks", *Computerworld*, US, available at: https://www.computerworld.com/article/2577244/top-10-vulnerabilities-in-today-s-wi-fi-networks.html
15. Podorozhniak, A., Liubchenko, N., Oliinyk, V. and Roh, V. (2023), "Research Application of the Spam Filtering and Spammer Detection Algorithms on Social Media and Messengers", *Advanced Information Systems*, Vol. 7, No. 3, pp. 60-66, doi: https://doi.org/10.20998/2522-9052.2023.3.09
16. Abdullah, Y. N. (2023), "Accuracy and Coverage Analysis of IP Geolocation Databases", *2023 International Balkan Conference on Communications and Networking* (BalkanCom), İstanbul, Turkiye, pp. 1–6. doi: https://doi.org/10.1109/BalkanCom58402.2023.10167899
17. Shmatko, O., Herasymov, S., Lysetskyi, Y., Yevseiev, S., Sievierinov O., Voitko, T., Zakharzhevskyi, A., Makogon, H., Nesterov, A. and Bondarenko, K. (2023), "Development of the automated decision-making system synthesis method in the management of information security channels", *Eastern-European Journal of Enterprise Technologies*, Vol. 6/9 (126), pp. 39–49, doi: https://doi.org/10.15587/1729-4061.2023.293511

18. Yevseiev, S., Hryshchuk, R., Molodetska, K. et. al. (2022), *Modeling of security systems for critical infrastructure facilities*, PC TECHNOLOGY CENTER, Kharkiv, 196 p., doi: https://doi.org/10.15587/978-617-7319-57-2
19. Kovalenko, A. and Kuchuk, H. (2022), "Methods to Manage Data in Self-healing Systems", *Studies in Systems, Decision and Control*, Vol. 425, pp. 113–171, doi: https://doi.org/10.1007/978-3-030-96546-4_3
20. Dotsenko, N., Chumachenko, I., Galkin, A., Kuchuk, H. and Chumachenko, D. (2023), "Modeling the Transformation of Configuration Management Processes in a Multi-Project Environment", *Sustainability (Switzerland)*, Vol. 15(19), 14308, doi: https://doi.org/10.3390/su151914308
21. (2016), "SMS Spam Collection Dataset: Collection of SMS messages tagged as spam or legitimate", *UCI MACHINE LEARNING*, available at: https://www.kaggle.com/uciml/sms-spam-collection-dataset
22. Jensen, G.G., Busch, M.B., Piovesan, M. And Haerter, J.O. (2023), "Nudging cooperation among agents in an experimental social network", *Applied Network Science*, Vol. 8(1), 62, doi: https://doi.org/10.1007/s41109-023-00588-x
23. Fennell, S.C., Gleeson, J.P., Quayle, M., Durrheim, K. and Burke, K. (2023), Agent-based null models for examining experimental social interaction networks, Scientific Reports, 13(1), 5249, doi: https://doi.org/10.1038/s41598-023-32295-z
24. Dun B., Zakovorotnyi, O. and Kuchuk, N. (2023), "Generating currency exchange rate data based on Quant-Gan model", *Advanced Information Systems*, Vol. 7, no. 2, pp. 68–74, doi: http://dx.doi.org/10.20998/2522-9052.2023.2.10
25. Gomathi, B., Saravana Balaji, B., Krishna Kumar, V., Abouhawwash, M., Aljahdali, S., Masud, M. and Kuchuk, N. (2022), "Multi-Objective Optimization of Energy Aware Virtual Machine Placement in Cloud Data Center", *Intelligent Automation and Soft Computing*, Vol. 33(3), pp. 1771–1785, doi: http://dx.doi.org/10.32604/iasc.2022.024052
26. (2023), *Python for Beginners. Python Software Foundation*, available at: https://www.python.org/about/gettingstarted/
27. Messaoudi, C., Romdhane, L.B. and Guessoum, Z. (2023), "AMIR: A Multi-agent Approach for Influence Detection in Social Networks", Lecture Notes in Networks and Systems, 740 LNNS, pp. 242–253, doi: http://dx.doi.org/10.1007/978-3-031-38333-5_25

Надійшла (received) 11.11.2023
Прийнята до друку (accepted for publication) 06.02.2024

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Герасимов Сергій Вікторович – доктор технічних наук, професор, начальник кафедри експлуатації озброєння та військової техніки, Військовий інститут танкових військ, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Serhii Herasymov – Doctor of Technical Sciences, Professor, Head of the Department of Weapons and Military Equipment Operation, Military Institute of Tank Troops, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: gsvnr@ukr.net; ORCID ID https://orcid.org/0000-0003-1810-0387;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57331504300.

Ткачов Андрій Михайлович – кандидат технічних наук, доцент, доцент кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Andrii Tkachov – Candidate of Technical Sciences, Associate Professor, Associate Professor of Cyber Security Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: snsncps@gmail.com; ORCID ID https://orcid.org/0000-0003-1428-0173;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57416821200.

Базарний Сергій Васильович – аспірант, Національний університет оборони України, Київ, Україна;
Sergii Bazarnyi – graduate student, The National Defense University of Ukraine, Kyiv, Ukraine;
e-mail: bazarnyisergii@gmail.com; ORCID ID http://orcid.org/0000-0001-9545-1960.

Комплексний метод визначення місцезнаходження агентів соціальних мереж в інтересах інформаційної операції

С. В. Герасимов, А. М. Ткачов, С. В. Базарний

Анотація. У дослідженні розроблено метод визначення місцезнаходження агентів соціальних мереж в інтересах проведення інформаційної операції на основі комплексного підходу аналізу даних інформаційної системи. **Актуальність методу** обумовлюється необхідністю уточнення цільової аудиторії противника в районі проведення інформаційної операції. **Авторами запропоновано** комплексний метод визначення місцезнаходження агентів соціальних мереж, який базується на поєднанні даних аналізу соціальних зв'язків визначеного агенту, геотегів та часу реєстрації його друзів у соціальній мережі, баз даних IP-адрес та геолокацій агентів соціальних мереж. Перевагою розробленого методу є можливість його застосування без безпосереднього доступу до пристроїв агентів соціальної мережі, що користуються даними супутникових систем глобального позиціонування. **Результати.** Запропонований комплексний метод визначення місцезнаходження агентів соціальних мереж в інтересах інформаційної операції включає такі основні етапи, як: знаходження множини друзів визначеного агенту соціальних мереж; знаходження IP кожного друга агента соціальних мереж з визначеної множини його друзів; за знайденими IP за допомогою баз даних геолокації IP визначається цільова аудиторія, у яку входять ті друзі агенту соціальної мережі, що мешкають у тому ж самому місті; для виключення впливу помилок у базах даних геолокації IP перевіряються місця реєстрацій друзів агенту соціальних мереж (за місцем та часом), чим визначається найбільш ймовірне їх постійне місцезнаходження; за результатом уточнення цільової аудиторії методом виключення тих агентів соціальної мережі, більшість реєстрацій яких є в інших місцях, формується підсумкова цільова аудиторія за ознакою однакового географічного місцезнаходження агентів соціальних мереж. **Висновок.** Застосування запропонованого комплексного методу визначення місцезнаходження агентів соціальних мереж дає можливість підвищити ефективність проведення інформаційних операцій за рахунок більш точного визначення цільової аудиторії противника в районі проведення операцій. Напрямком удосконалення розробленого методу може бути його інтеграція з комплексними інформаційними системами психологічного впливу, а також використання методів та алгоритмів машинного навчання.

Ключові слова: агенти соціальних мереж; геолокація; геотег, інформаційна система; цільова аудиторія; психологічний вплив.