UDC 004.056.55 **doi:** https://doi.org/10.20998/3083-6298.2025.02.02

Kateryna Vashchuk[1], Andrii Astrakhantsev[1]

[1] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine

ASSESSMENT OF USER SECURITY BASED ON OSINT METHODS IN INFORMATION AND COMMUNICATION NETWORKS

Abstract. Topicality. In the modern information society, open data access plays a critical role in decision-making in areas such as security, business, and analytics. One of the most promising approaches is Open Source Intelligence (OSINT), which enables the collection, processing, and use of publicly available information from the Internet, media, and social networks. The growing volume of digital data creates both opportunities and challenges for ensuring user privacy and security. **The subject of study** in the article is methods of collecting, analyzing, and verifying open information about users of information and communication networks using OSINT tools, with particular attention to the impact of privacy settings on the effectiveness of data gathering. **The purpose of the article** is to assess the security levels of users based on OSINT methods and to develop a web application for automated search and preliminary analysis of user data. **The following results** were obtained. Three categories of Telegram users (low, medium, and high privacy) were analyzed. A set of OSINT tools –WhatsMyName, Sherlock, Namecheckr, and others – was applied to identify accounts, track digital footprints, and verify metadata. Special attention was given to reverse image search and geolocation techniques for profile photo analysis. The developed application implements modules for username-based search, email verification, and combined analysis, which enhance the efficiency of OSINT investigations. **Conclusion.** The developed application can be applied in cybersecurity, law enforcement, and corporate security to improve digital safety strategies and user privacy practices.

Keywords: OSINT; open sources; information security; digital footprint; data analysis; user privacy; cybersecurity.

Introduction

Problem relevance. In today's information society, data has become one of the key factors influencing decision-making in areas such as security, business intelligence, and analytics. Open Source Intelligence (OSINT) – the practice of gathering, analyzing, and utilizing information from publicly accessible sources such as the Internet, mass media, and social networks – plays an increasingly significant role in modern cybersecurity and investigative practices [1,2,3,15]. Unlike traditional intelligence methods, OSINT relies solely on legally accessible data, which makes it especially important in the context of counter-terrorism, criminal investigation, and corporate security [13, 14].

Literature review. Numerous studies highlight the importance of OSINT in modern security operations, particularly in the areas of cyber threat detection, online privacy measurement, and automation of investigative processes [4,9,10,12]. Sources such as the OSINT Framework [1] and Bazzell's "Open Source Intelligence Techniques" [2] provide structured methodologies for information gathering, while Renaud [4] addresses the measurement of digital footprints to raise privacy awareness. However, existing research often overlooks the correlation between online privacy settings and the efficiency of OSINT-based information gathering, leaving a gap in the evaluation of practical privacy impacts on investigative outcomes.

Purpose of the research. The aim of this work is to assess user security levels in information and communication networks by applying OSINT techniques, with a focus on the relationship between privacy settings and the exposure of personal data. The study also includes the development of a specialized web-based OSINT application that automates the search and preliminary analysis of user information, integrating APIs from platforms such as GitHub [5], Twitter [6], Hunter.io [7], Reddit and Telegram [8], enabling efficient, structured, and legally compliant data collection for investigative and cybersecurity purposes.

1. Research techniques

This paper applies OSINT techniques to analyze the privacy exposure of three types of Telegram [8] user profiles with different privacy configurations. The process follows the OSINT cycle [11] – from planning and scoping to data gathering, verification, and reporting – and aims to assess how privacy settings impact the availability of personal data in open sources. (Fig.1).

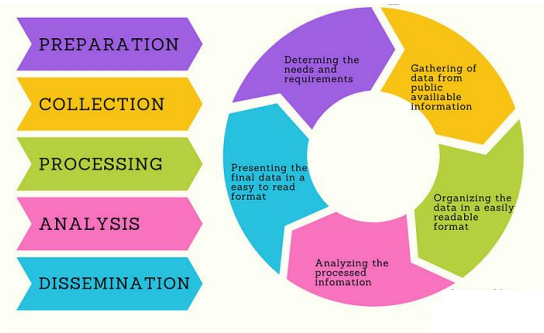

Fig.1. OSINT cycle [11]

1.1. User Profiles and Privacy Levels. To evaluate the impact of privacy configurations on data exposure, three representative Telegram user profiles were selected for analysis. The categorization was based on the availability of personal information and visibility of profile attributes in open sources. These profiles

illustrate different approaches to privacy settings and their effectiveness in limiting OSINT-based data gathering (Table 1).

Table 1 – **Observable data by Telegram privacy level**

Publicly Available Personal Data	*User A (Low Privacy Level)*	*User B (Medium Privacy Level)*	*User C (High Privacy Level)*
Public Username	✓	✓	✓
Open Access to Phone Number	✓	✗	✗
Public Profile Photo	✓	✓	✗
Open Biography with Personal Information	✓	✗	✗

From Table 1 it is clear that:

- Profile A – Low Privacy: Public username, profile photo, and numerous cross-platform accounts.
- Profile B – Medium Privacy: Public username with limited visible data, moderate restrictions on information.
- Profile C – High Privacy: Minimal publicly available data, no profile photo, few platform associations.

The comparative characteristics of these profiles are summarized in Table 1, which highlights the observable data points for each privacy level.

1.2. Data Collection Tools and APIs. For the OSINT investigation, an integrated approach combining specialized utilities, public APIs, and reverse image search services was employed. Username enumeration was conducted using tools such as WhatsMyName, Sherlock, Namecheckr, Namecheckup, and UserSearch.org. Public API integrations included GitHub [5], Twitter [6], Reddit, Hunter.io [7], and Telegram Search [8]. Reverse image analysis was performed through TinEye, Picarta, and Bing Visual Search. The overall architecture of the OSINT investigation framework, integrating all applied utilities, APIs, and image search services, is illustrated in Fig 2.

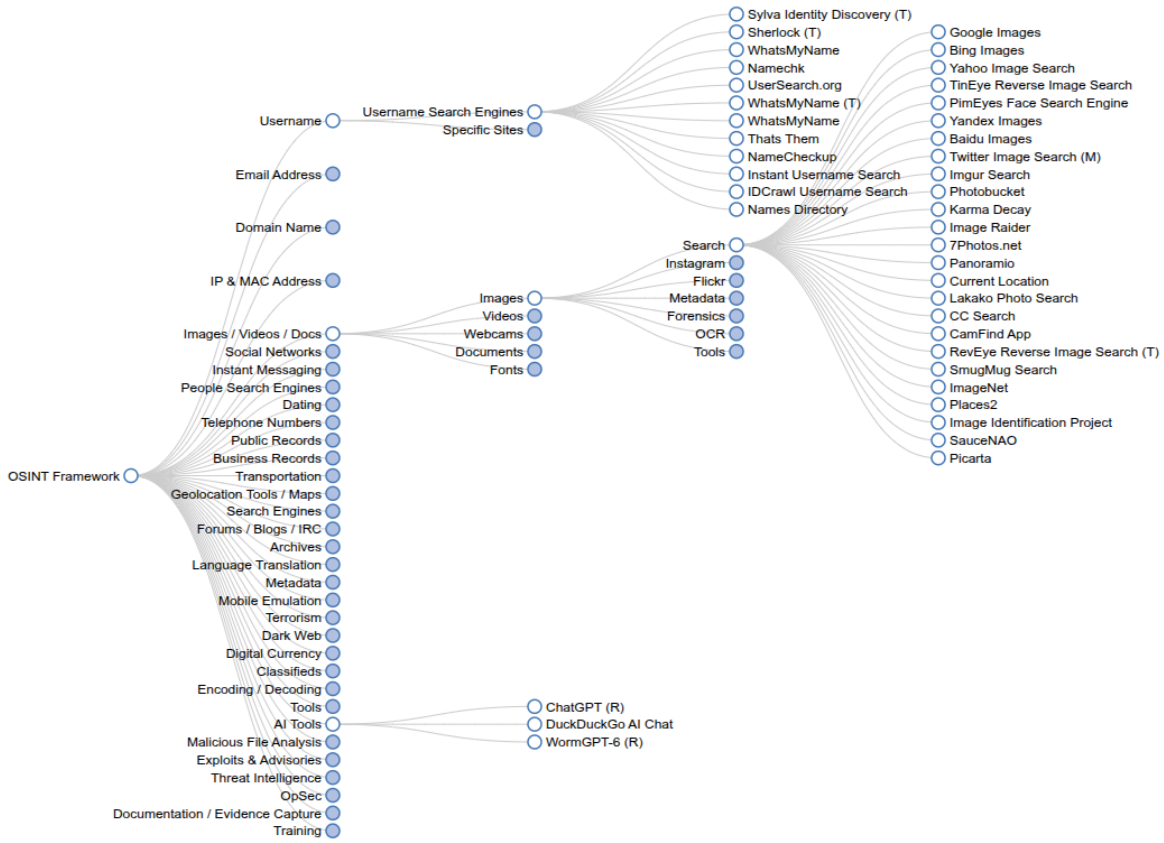

Fig.2. OSINT framework with integrated utilities and APIs

2. Results of research

2.1. Findings per Profile. Profile A (Fig.3) – Low Privacy The analysis revealed extensive cross-platform presence. Multiple matches were found on GitHub, Twitter, Reddit, Pinterest, and Medium. Reverse image search suggested possible geolocation in the Carpathian region. Based on timestamps and activity logs, behavioral patterns and timelines of online presence were reconstructed.

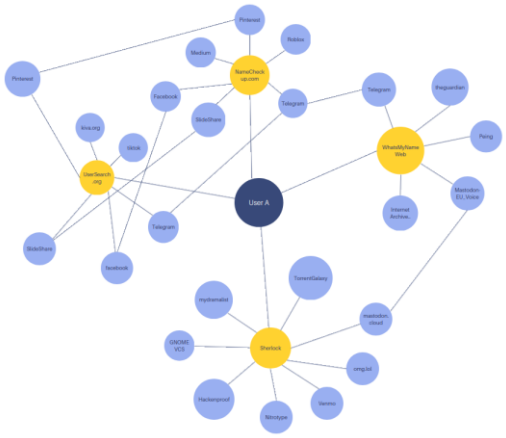

Fig.3. Profile A example – Low Privacy

Profile B (Fig.4) – Medium Privacy Search results included matches on GitLab, Mastodon, Pinterest, and various freelance platforms. Reverse image search indicated a possible geolocation in the Czech Republic, but the volume of identifiable traces was noticeably smaller compared to Profile A.

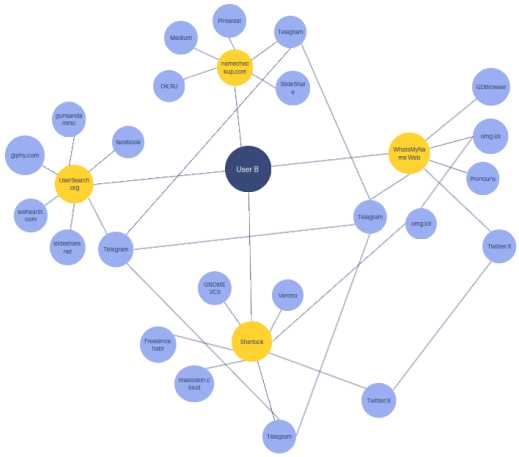

Fig.4. Profile B example – Medium Privacy

Profile C (Fig.5) – High Privacy Only limited matches were detected, primarily anonymous or inactive accounts. While minimal cross-platform correlation was found, some traces existed on Reddit and GitHub. No high-confidence geolocation was established.

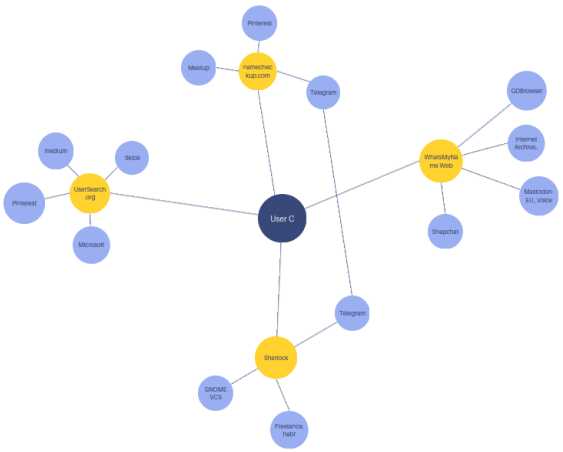

Fig.5. Profile C example – High Privacy

2.2. Summary of Results. The comparative analysis based on actual OSINT investigation data shows a clear correlation between privacy settings and the volume of publicly accessible information (Fig. 6):

- Low Privacy (User A) – 25 detected username mentions (100% baseline). The profile allowed for extensive cross-platform correlation, geolocation inference, and behavioral pattern reconstruction.
- Medium Privacy (User B) – 23 mentions (92% of baseline), resulting in an 8% reduction in observable data. While most platforms were still discoverable, certain sensitive traces were obscured.
- High Privacy (User C) – 13 mentions (52% of baseline), a 48% reduction in observable data. Minimal public footprint significantly limited OSINT possibilities, although complete anonymity was not achieved.

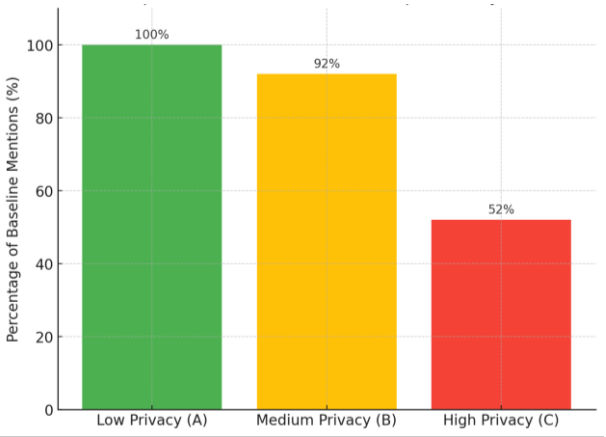

Fig. 6. Comparative Chart of Data Volume per Privacy Level

Overall, raising the privacy level from low to high resulted in an average exposure reduction of 24%. This confirms that privacy-conscious behavior substantially reduces OSINT discovery potential, yet cannot entirely prevent data leaks.

3. Transition to Java Application Implementation

The findings from this analysis provided the foundation for the development of a custom Java-based OSINT automation tool. This application integrates the previously mentioned utilities and APIs [5 - 8], enabling automated data collection, normalization, and report generation for different privacy profiles. The next section describes the design, architecture, and implementation details of this Java application, illustrating how the research methodology was transformed into a functional investigative framework.

3.1. Purpose and Scope. The application focuses on two core OSINT methods identified as highly effective during the research phase:

- Username search across multiple online platforms – By systematically querying several specialized tools and APIs [5-8], the application can detect cross-platform account matches for a given username. This approach enables the identification of linked accounts, potential aliases, and activity traces across diverse services, which would otherwise require considerable manual effort.
- Email verification via public API services – Using trusted APIs such as Hunter.io [7], the system can quickly verify whether an email address is valid, discover associated domains, and identify potential patterns in registration data. This process allows investigators to confirm the authenticity of contact information and detect possible fraudulent or disposable addresses.

Unlike the manual OSINT process, where each lookup must be performed individually, the Java application executes these operations automatically, in parallel, drastically reducing the time needed for data gathering. Moreover, it ensures consistency in search results, eliminates human oversight in repetitive checks, and supports batch processing, making it suitable for large-scale investigations. This automation not only accelerates the workflow but also standardizes the output, allowing for more efficient data analysis and reporting.

3.2. System Architecture and Workflow. Based on the results of the comparative analysis in Section 5, the development of the Java OSINT automation tool focused on streamlining the two most effective investigative methods: username search and email verification. The application was built with a modular architecture, ensuring that each function is clearly separated for maintainability and allowing the system to be expanded in the future without major structural changes.

The process begins when the operator provides an input - either a username or an email address - which can be entered manually or loaded from a prepared file. Once the input is received, the system automatically initiates queries to a selected set of social platform APIs [5–7,13,14], chosen during the research phase as the most informative for OSINT purposes. For email addresses, the tool integrates with public verification services such as Hunter.io [7] to confirm their validity and retrieve any additional metadata available from open sources.

All collected data then passes through a normalization layer that unifies different API responses into a consistent format, eliminating discrepancies and preparing the information for analysis. The final stage of the workflow is automated report generation, in which the processed results are exported in structured format such as JSON. This allows investigators to easily review, archive, or integrate the findings into other analytical tools.

By automating these stages, the application eliminates repetitive manual tasks, reduces the time required for searches, and ensures consistent data formatting. Compared to the manual OSINT workflow described in earlier sections, this approach enables faster, more reliable, and more scalable investigations while minimizing the risk of human error.

3.3. Advantages of the Automated Approach. The transition from a manual OSINT process to a fully automated Java application significantly improved the efficiency and consistency of investigations. In manual mode, each username or email required separate queries to multiple platforms, manual parsing of results, and manual report formatting - a process prone to delays and human error. The automation removed these bottlenecks by executing all configured searches in parallel, unifying data structures on the fly, and generating ready-to-use reports instantly.

This approach not only reduced the total investigation time but also ensured that results were formatted in a consistent way, enabling quick comparison between cases. Additionally, the modular design allows the application to scale efficiently - supporting bulk processing of dozens or even hundreds of inputs without compromising accuracy. The reduced reliance on human operators also minimizes the likelihood of overlooking critical data points, which can be crucial in high-stakes OSINT scenarios.

3.4. Performance Overview. To evaluate the efficiency of the developed Java OSINT automation tool, comparative timing tests were carried out against the original manual investigation process. The scenario included processing a batch of 20 mixed queries — usernames and email addresses — using both methods.

The automated system completed all queries in under 2 minutes, while the manual approach took approximately 25 minutes (Fig. 7). This translates to a time reduction of more than 90%, without compromising accuracy. In fact, direct API integration and parallel request execution occasionally improved the completeness of results, reducing the chance of missed data sources.

The performance gain was especially visible in username searches, where the application handled requests almost instantly compared to the prolonged manual browsing of multiple platforms. Email verification checks also benefited from automation, enabling rapid validation via API calls instead of manual copy-pasting and formatting.

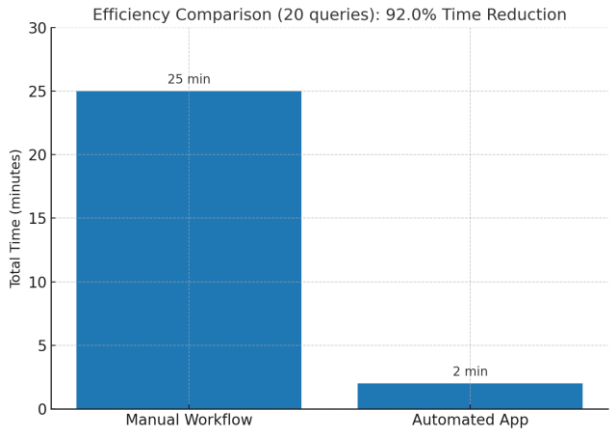

Fig. 7. Efficiency comparison chart: manual vs automated search time

The performance results are illustrated in Fig. 7, which clearly demonstrates the difference in total processing time between manual and automated workflows.

4. Discussion of results

The conducted study highlights both the scientific and practical significance of assessing user security through OSINT methods in information and communication networks. The analysis of user profiles and privacy levels confirmed that even limited public exposure of personal information can significantly increase security risks, especially when combined with automated data collection tools and APIs. The findings per profile demonstrate how fragmented user data can be systematically aggregated into a comprehensive digital footprint, thereby revealing potential vulnerabilities that would otherwise remain unnoticed.

The transition to a Java-based application implementation and the design of a corresponding system architecture and workflow illustrate the feasibility of translating theoretical models into a functional software solution. This integration not only provides a practical tool for cybersecurity specialists but also serves as a framework for further research into automated OSINT-based security assessments.

The performance evaluation confirmed that the automated approach is capable of scaling across large datasets with high efficiency, thereby demonstrating advantages over traditional manual analysis. This positions the proposed system as a valuable contribution for both academia and industry in enhancing user security awareness and strengthening proactive defense mechanisms.

Future research directions include the incorporation of machine learning techniques for risk prediction, the extension of data sources to encompass more diverse platforms, and the integration of privacy-preserving mechanisms to ensure ethical compliance in OSINT investigations. Additionally, refining the architecture for deployment in real-world security operations centers (SOCs) may further enhance its applicability.

5. Conclusion

The conducted research demonstrated a clear relationship between user privacy settings and the amount of data accessible through OSINT methods. Comparative analysis of three test profiles confirmed that higher privacy levels lead to a significant reduction in publicly available information — up to 48% compared to low-privacy configurations — while complete anonymity remains unattainable.

Building on these findings, a custom Java-based OSINT automation tool was developed to address the limitations of manual investigation workflows. By automating username searches and email verification, the tool reduced processing time by over 90% and ensured greater consistency and scalability of results.

The implemented system architecture allows for easy integration of additional APIs, making the solution adaptable to evolving OSINT requirements. Future improvements may include expanding the supported data sources, adding sentiment or behavioral analysis, and implementing advanced reporting capabilities.

Ultimately, this work bridges theoretical OSINT methodology with practical, automated implementation — providing a foundation for more efficient and precise open-source investigations while emphasizing the importance of privacy awareness in the digital environment.

REFERENCES

1. OSINT Framework, [online]. https://osintframework.com
2. Bazzell, M. (2021), “Open Source Intelligence Techniques”, *7th ed., IntelTechniques*, [online]. https://ru.scribd.com/document/550389983/Michael-Bazzell-Open-Source-Intelligence-Techniques-Resources-for-Searching-and-Analyzing-Online-Information-Createspace-Independent-Publishing-Pla
3. Clark, J. (2020), “OSINT Techniques: Resources for Investigating Individuals”, *CreateSpace Independent Publishing.*
4. Renaud, K. (2020), “Measuring Digital Footprints for Online Privacy Awareness”, *Journal of Cybersecurity*, vol. 6, no. 1, pp. 1–14.
5. GitHub API Documentation, [online]. https://docs.github.com/en/rest
6. Twitter Developer Docs, [online]. https://developer.twitter.com/en/docs
7. Hunter.io API Documentation, [online]. https://hunter.io/api
8. Telegram username search, [online]. https://core.telegram.org/
9. OWASP Foundation (2021), “OWASP Top 10 Security Risks”, [online]. https://owasp.org
10. Newman, S. (2021), “Building Microservices: Designing Fine-Grained Systems”, *2nd ed., O’Reilly Media.*

11. OSINT Team (2023), “The OSINT Cycle: Getting Familiar with the Process of Data Collection and Analysis”, *OSINT Team Blog,* [online]. https://osintteam.blog/the-osint-cycle-getting-familiar-with-the-process-of-data-collection-and-analysis-day3-of-6f53fcdb4234
12. Molfar (2024), “What is OSINT in 2024: A Guide from Molfar”, [online]. https://molfar.com/blog/shcho-take-osint-u-2024-gaid-vid-molfar
13. Europol (2021), “New trace object uploads – fresh leads needed in child sexual abuse cold cases”, *Europol Official Website,* [online]. https://www.europol.europa.eu/media-press/newsroom/news/new-trace-object-uploads-fresh-leads-needed-in-child-sexual-abuse-cold-cases
14. Higgins, E. (2015), “MH17: The Open Source Evidence”, [online]. https://www.bellingcat.com/app/uploads/2015/10/MH17-The-Open-Source-Evidence-EN.pdf
15. Greenberg, A. (2020), “How the Alleged Twitter Hackers Got Caught”, *WIRED*, [online]. https://www.wired.com/story/how-alleged-twitter-hackers-got-caught-bitcoin

Received (Надійшла) 18.08.2025
Accepted for publication (Прийнята до друку) 29.08.2025

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

Ващук Катерина Василівна – магістр, Національний технічний університет України “Київський політехнічний інститут ім. Ігоря Сікорського”, Київ, Україна;
Kateryna Vashchuk – master-student, “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine;
e-mail: clahfclns@gmail.com; ORCID Author ID: https://orcid.org/0009-0006-9631-3176

Астраханцев Андрій Анатолійович – доктор технічних наук, доцент, Національний технічний університет України “Київський політехнічний інститут ім. Ігоря Сікорського”, Київ, Україна;
Andrii Astrakhantsev – Doctor of Technical Sciences, Associate Professor, “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine;
e-mail: andrii.astrakhantsev@nure.ua; ORCID Author ID: https://orcid.org/ 0000-0002-6664-3653;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId= 55226016400.

ОЦІНКА БЕЗПЕКИ КОРИСТУВАЧІВ НА ОСНОВІ МЕТОДІВ OSINT В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖАХ

К. В. Ващук, А. А. Астраханцев

Анотація. Актуальність. У сучасному інформаційному суспільстві доступ до відкритих даних відіграє вирішальну роль у прийнятті рішень у таких сферах, як безпека, бізнес та аналітика. Одним із найперспективніших підходів є розвідка з відкритим кодом (OSINT), яка дозволяє збирати, обробляти та використовувати загальнодоступну інформацію з Інтернету, ЗМІ та соціальних мереж. Зростаючий обсяг цифрових даних створює як можливості, так і виклики для забезпечення конфіденційності та безпеки користувачів. **Предметом дослідження** у статті є методи збору, аналізу та перевірки відкритої інформації про користувачів інформаційно-комунікаційних мереж за допомогою інструментів OSINT, з особливою увагою до впливу налаштувань конфіденційності на ефективність збору даних. **Метою статті** є оцінка рівнів безпеки користувачів на основі методів OSINT та розробка веб-додатку для автоматизованого пошуку та попереднього аналізу даних користувачів. Отримані **наступні результати**. Проаналізовано три категорії користувачів Telegram (низький, середній та високий рівень конфіденційності). Для ідентифікації облікових записів, відстеження цифрових слідів та перевірки метаданих застосовано набір інструментів OSINT – WhatsMyName, Sherlock, Namecheckr та інші. Особлива увага приділена методам зворотного пошуку зображень та геолокації для аналізу фотографій профілю. Розроблений застосунок реалізує модулі для пошуку за іменем користувача, перевірки електронної пошти та комбінованого аналізу, що підвищує ефективність OSINT-розслідувань. **Висновки.** Розроблений застосунок може бути застосований у кібербезпеці, правоохоронних органах та корпоративній безпеці для покращення стратегій цифрової безпеки та практик конфіденційності користувачів.

Ключові слова: OSINT; відкриті джерела; інформаційна безпека; цифровий слід; аналіз даних; конфіденційність користувачів; кібербезпека.