UDC: 004.056/.57:004.8:519.87OSINT
DOI: https://doi.org/10.17721/ISTS.2024.8.49-55

Laryisa DAKOVA, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0001-6104-8217
e-mail: dacova@ukr.net
State University of Information and Communication Technologies, Kyiv, Ukraine

Maryana LEVYTSKA, Student
ORCID ID: 0009-0007-1617-029X
e-mail: levytskam@fit.knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Katerina HAVENKO, Student
ORCID ID: 0009-0005-7036-9318
e-mail: havenkok@fit.knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

USAGE OF OPEN-SOURCE INTELLIGENCE FOR SECURITY OF CRITICAL INFRASTRUCTURE

Background. ***In the metter of critical infrastructure, it refers to the systems and assets that are essential for the functioning of modern society and the economy. These sectors include energy, transportation, elecommunications, healthcare, and water supply, all of which are crucial for national security and public well-being. Disruptions in these infrastructures can lead to decent amount of social and economic vital consequences.***

With the technologies happening to become more advanced, critical infrastructure security systems have become more complex and affiliated. Alterations in example being smart grids, automated transportation systems, and sophisticated communication networks have enhanced efficiency but also increased vulnerabilities. The convergence of digital and physical systems makes these sectors more exposed to risks like cyberattacks, natural disasters, terrorism, and other threats. This growing complexity emphasizes the need for governments and organizations to prioritize the protection of these vital infrastructures.

Methods. ***In this research, we developed a mathematically rigorous approach to OSINT in the protection of critical infrastructure, improving on existing methods by providing a structured model for threat detection, vulnerability assessment, and risk calculation. The proposed method employs mathematical representations and probability functions, ensuring a more accurate analysis of threat information and vulnerability scoring. This advancement enables more precise mitigation strategies and better response coordination. While existing OSINT methods rely heavily on unstructured data collection and analysis, our approach introduces a mathematical foundation for data gathering and threat evaluation, providing several key improvements, such as Mathematical Representation of Data; Probabilistic Threat Detection and Vulnerability and Risk Assessment with Weighted Metrics.***

Results. ***The study's findings underscore the value of a quantitative OSINT model in critical infrastructure security, demonstrating improvements in accuracy, speed, and decision-making. By reducing ambiguity through probabilistic risk assessments, the model minimizes unnecessary alerts and focuses on actionable threats. Scalability testing showed the model could handle large datasets effectively without overwhelming analysts. Finally, objective risk assessments were validated as enhancing decision-making processes, thus proving beneficial in real-time threat detection and mitigation. The model provides a solid foundation for continuously evolving OSINT practices and suggests potential for further optimization by minimizing risk and balancing mitigation efforts through a defined objective function.***

Conclusions. ***After all conducted analytical works, we could definitely say that this mathematical model demonstrates how OSINT can be systematically used to enhance the security of critical infrastructure by assessing vulnerabilities, detecting threats, calculating risk, and applying targeted mitigation strategies. It leverages data collection from open sources, threat analysis, and continuous feedback to ensure that infrastructure systems are resilient to evolving risks.***

Keywords: ***OSINT, critical infrastructure security, cyber threats, vulnerability assessment, infrastructure resilience, public sources, data analysis, cybersecurity, information security.***

Background

Open-source intelligence (OSINT) consists of targeted information that is gathered and organized in a specific manner to address particular questions.

This concept evolved from the term "information from open sources" (Open Source Information). In its simplest form, it refers to information that is not classified as "secret." The U.S. Intelligence Community defines this type of information as "publicly available material that can be legally acquired through requests, purchases, or observation, while adhering to copyright protection regulations".

The basis of intelligence gathering is research, which appears to be a verified intelligence requirements with existing sources in order to create a product that fulfills vital needs. This general approach to the collection is the equal way applicable to already classified sources as it is to open sources.

The aim of this work is to investigated the contribution of Open-Source Intelligence to the protection of critical infrastructure. OSINT involves the collection and analysis of publicly accessible data, such as content from social media platforms, news articles and web services. The research highlights how OSINT can be utilized to pinpoint potential security gaps, examine risks, and upgrade and develop responses to emerging threats in critical sectors like energy, transportation, telecommunications, and utilities.

Figure 1 below shows an overview of the elements of the Open Intelligence Collection (OSINT) process.

Background and Importance of the Security of Critical Infrastructure. In the metter of critical infrastructure, it refers to the systems and assets that are essential for the functioning of modern society and the economy. These sectors include energy, transportation, elecommunications, healthcare, and water supply, all of which are crucial for national security and public well-being. Disruptions in these infrastructures can lead to decent amount of social and economic vital consequences (Clarke, 2011; Best, 2011; MTLS, 2010).

With the technologies happening to become more advanced, critical infrastructure security systems have become more complex and affiliated. Alterations in example being smart grids, automated transportation systems, and sophisticated communication networks have enhanced efficiency but also increased vulnerabilities. The convergence of digital and physical systems makes these sectors more exposed to risks like cyberattacks, natural disasters, terrorism, and other threats. This growing complexity emphasizes the need for governments and organizations to prioritize the protection of these vital infrastructures (Clarke, 2011; Lowenthal, 2017; Brown, 2010).

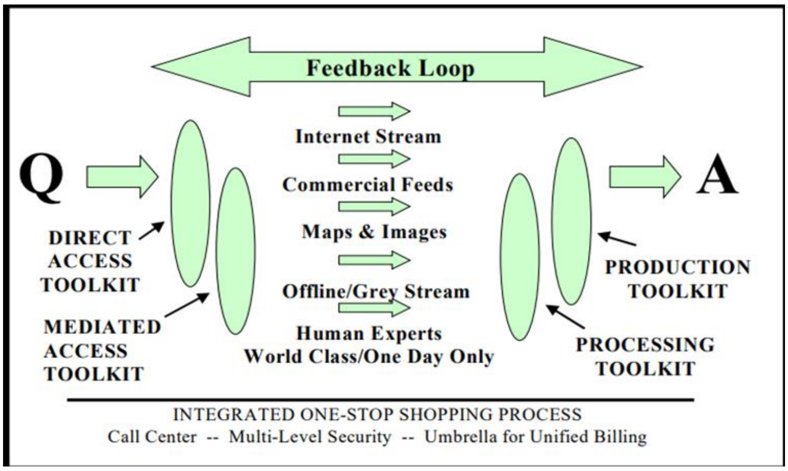

Fig. 1. OSINT collection process (Congressional Research Service, 2007; NATO, 2001)

The increasing complexity and interconnectedness of modern infrastructure. Open-Source Intelligence gathering and analyzing information that is publicly and legally available from sources such as the internet, social media, academic publications, government documents, and press releases. In the context of critical infrastructure security, OSINT plays a key role in identifying potential threats and vulnerabilities. It also brings to light often overlooked information that can help improve the security of these essential assets (Congressional Research Service, 2007; NATO, 2001; Lowenthal, 2017).

The use of OSINT has gained increasing acceptance in modern security practices, largely due to the vast amount of publicly available data. With the right tools, this data can be gathered quickly, enabling more effective risk management. OSINT complements traditional intelligence methods, enhancing situational awareness and enabling more accurate, forward-looking threat assessments (Lowenthal, 2017; Best, 2011; Mutschke, 2018).

Role of Open-Source Intelligence. OSINT, or Open-Source Intelligence, is a type of intelligence gathered by collecting and analyzing data from widely available sources. Comparing to classified intelligence, which relies on confidential data accessible to only a limited group, OSINT draws from sources like the news, social media platforms, government reports, academic research, and public records. What makes OSINT unique is that it's not just about gathering data – it's about processing and applying it to real-world situations (Congressional Research Service, 2007; NATO, 2001; Best, 2011).

In the security field, OSINT pulls information from a variety of sources, such as traditional media and social networks like Facebook, to help spot emerging risks or changes in the environment (NATO, 2001) and (Levytska, 2024; Lowenthal, 2017). By continuously monitoring and analyzing these sources, OSINT helps achieve security goals while staying within legal and ethical limits (Clarke, 2011; Best, 2011). As global infrastructure becomes more interconnected and complex, the importance of open-source intelligence is becoming increasingly important in modern security systems (Congressional Research Service, 2007; Lowenthal, 2017; Brown, 2010). The huge amounts of data available online, along with advances in technology, allow this information to be shared and accessed quickly (Best, 2011; Brown, 2010; Zegart, 2015).

These sources can include:

- News articles, television reports, and radio broadcasts (Lowenthal, 2017).
- Websites, blogs, forums, and online databases (Best, 2011).
- Media Platforms like Twitter (X), Instagram, Facebook LinkedIn, and others where users generate huge amounts of real-time data (Schafer, 2017; Knight, 2020).
- Official government publications, research, and statistical data released by governments.
- Academic papers, dissertations, and journals published by universities and research institutions.
- Reports and data collected and shared by Non-Governmental Organizations.
- Maps, satellite images, and geographic data (Lewis, 2021).

The goal of OSINT is to turn raw, unstructured public data into useful intelligence that can support a range of activities, from national security efforts to corporate risk management. By using OSINT, organizations can spot potential threats, uncover vulnerabilities, and gain valuable insights into security challenges (Brown, 2010; Harding, 2019; Knight, 2020).

Since OSINT relies solely on information that's publicly available, it operates within legal and ethical boundaries. This makes it a cost-effective and flexible option for gathering intelligence compared to more traditional methods (NATO, 2001; Clarke, 2011; Lowenthal, 2017). It's used across many fields, such as cybersecurity, defense, law enforcement, and corporate security, to keep an eye on and respond to emerging risks (Lowenthal, 2017; Harding, 2019; Knight, 2020).

What makes OSINT even more powerful is the use of advanced techniques like data mining, monitoring of social media platforms, and natural language processing (NLP). These help sort through and analyze large amounts of data (Mutschke, 2018; Johnson, 2019), allowing OSINT experts to find the most meaningful insights from the flood of information that's constantly being generated (Mutschke, 2018; Schafer, 2017; Johnson, 2019).

In today's highly connected world, where data is being created and shared every second, OSINT has become increasingly important in ensuring quick and effective risk management and security responses.

Methods

This Fig. 2 represents the process of using Open-Source Intelligence techniques to gather, analyze, and extract meaningful insights from publicly available information, especially for purposes like security analysis and investigative work.

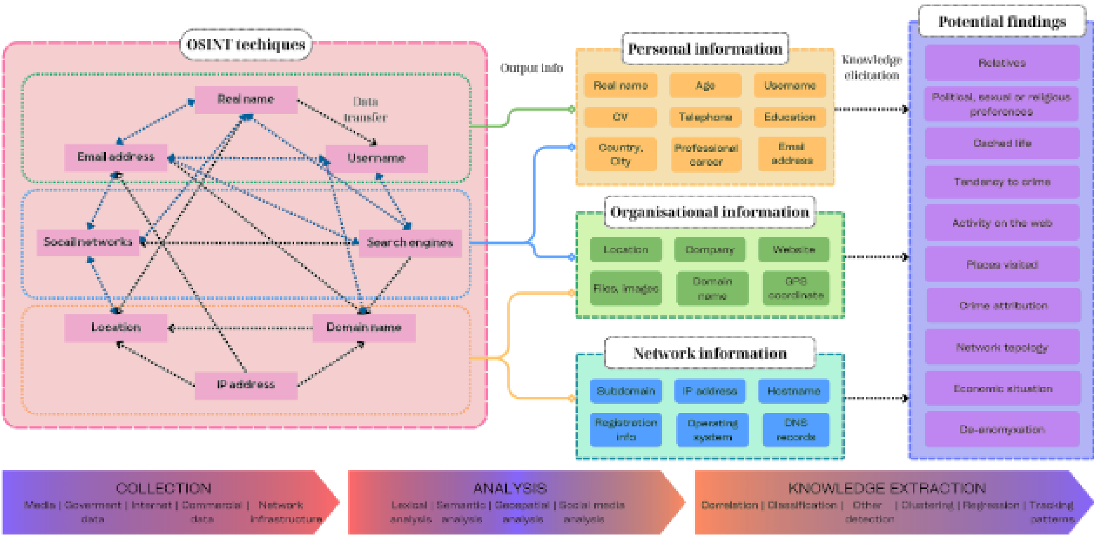

Fig. 2. OSINT collection process (Congressional Research Service, 2007; NATO, 2001)

OSINT Techniques and Data Collection

At the core of the Fig. 2, we can observe a network of interconnected OSINT techniques used to collect data from various sources. These techniques involve gathering details such as:

- Real names,
- Email addresses,
- Usernames,
- Social networks,
- Search engines,
- Location,
- Domain names, and IP addresses.

The Fig. 2 shows how these different pieces of information interact with one another, represented by arrows connecting the elements. For instance, a social network profile might reveal a person's real name or email address, while a search engine might help link a username to additional data, such as a social media profile or location information. Similarly, tracking an IP address might provide information about the user's location or the domain name they are associated with. This interplay highlights the richness of OSINT data, where one piece of information can lead to others, creating a web of connections that can be further explored.

Output Information

Once the data is collected, it is categorized into three main types of output information:

1. Sensitive Information, including details as an example person's real name, age, username, telephone number, education, email address, professional career, and location (city and country). This information is destructive for building profiles of individuals or groups.

2. Commercial Information, which relates to details about a company or organization, such as its location, website, domain name, GPS coordinates, and any associated files or images. Use such type of information can potentially help to understand an organization's structure, physical presence, and online footprint.

3. Network Information, which provides technical details, such as subdomains, IP addresses, hostnames, operating systems, DNS records, and registration information. This type of data is essential for building out the technical infrastructure of an person or an organization, and for understanding their presence in cyberspace.

Knowledge Elicitation and Potential Findings

The Fig. 2 further illustrates how the output information can be used for knowledge elicitation, producing a wide range of potential findings. These findings can reveal important insights, including:

- Personal connections, such as identifying relatives or close associates,
- Preferences, including political, sexual, or religious views,
- Cached life, referring to historical information that remains on the web,
- Tendency to commit crimes based on behavioral patterns,
- Web activity, identifying what individuals or groups are doing online,
- Places visited, through location data or travel histories,
- Crime attribution, linking individuals to potential criminal activities,
- Network topology, which helps understand the structure of a network,
- Economic situation, which can give insights into financial health or business activities,
- De-anonymization, which uncovers the identity of users who may be operating under the assumption of anonymity.

Analysis and Knowledge Extraction

At the bottom of the Fig. 2 we can observe outlined process of analysis, which involves several types of data processing:

- Lexical and semantic analysis focuses on understanding the meaning and context of textual data,
- Geospatial analysis uses geographic data, such as GPS coordinates, to track locations and movements,

- Social media analysis helps uncover relationships and patterns of behavior on platforms like Facebook, Twitter, or LinkedIn.

Finally, after the data has been analyzed, the process moves to knowledge extraction, where advanced techniques like correlation, classification, clustering, regression, and pattern tracking are used. This step involves extracting actionable intelligence by finding connections between evidently extraneous pieces of data, categorizing information, and identifying patterns over time. These methods allow investigators or security professionals to detect threats, track suspicious behavior, and make informed decisions based on OSINT findings.

Application to Critical Infrastructure Security

In the context of securing critical infrastructure, this process of OSINT monitoring and analysis can be instrumental. By gathering data from open sources such as social networks, websites, and public databases, security professionals can monitor for potential threats. For example, OSINT can help identify suspicious activity near sensitive infrastructure, uncover the digital footprints of individuals or organizations involved in planning attacks, or detect patterns in network behavior that indicate a cybersecurity breach. The ability to extract knowledge from OSINT enables authorities to respond proactively, strengthening the protection of vital systems.

This framework highlights the value of open-source intelligence in modern security operations, demonstrating how a variety of data sources and analysis techniques can be integrated to enhance situational awareness and threat detection.

Advanced OSINT Methodologies for Critical Infrastructure Security

What We Have Developed

In this research, we developed a mathematically rigorous approach to OSINT in the protection of critical infrastructure, improving on existing methods by providing a structured model for threat detection, vulnerability assessment, and risk calculation. The proposed method employs mathematical representations and probability functions, ensuring a more accurate analysis of threat information and vulnerability scoring. This advancement enables more precise mitigation strategies and better response coordination.

Comparison with Existing Methods

While existing OSINT methods rely heavily on unstructured data collection and analysis, our approach introduces a mathematical foundation for data gathering and threat evaluation, providing several key improvements:

Mathematical Representation of Data: Existing methods often involve ad hoc collection and manual filtering of data from open sources, which can lead to inaccuracies due to human error or noise. Our model formalizes the data collection process through the formula (1), ensuring that all relevant data points are systematically accounted for, reducing the possibility of missing critical information.

Probabilistic Threat Detection: Traditional threat detection methods may rely on keyword matching or expert analysis. However, these approaches do not quantify the likelihood of a true threat. We introduced a probability function (3.4.1) that mathematically evaluates the relevance of data to specific threats, offering a more reliable means of identifying real risks. This probabilistic approach reduces false positives and ensures a higher rate of accurate threat detection.

Vulnerability and Risk Assessment with Weighted Metrics: Current OSINT vulnerability assessments lack a formalized scoring system for infrastructure components. Our vulnerability scoring model (3.5.1) assigns specific vulnerability scores based on exposure to open-source threats, ensuring a quantitative and comparative analysis of different components. Furthermore, the risk score calculation (3.6.1) combines vulnerability and threat impact factors into a weighted function, allowing for more nuanced prioritization of critical risks.

To better understand the improvements offered by our method, we will now present the key mathematical models, visually on Fig. 3 and also mathematicaly below, that underpin our OSINT framework.

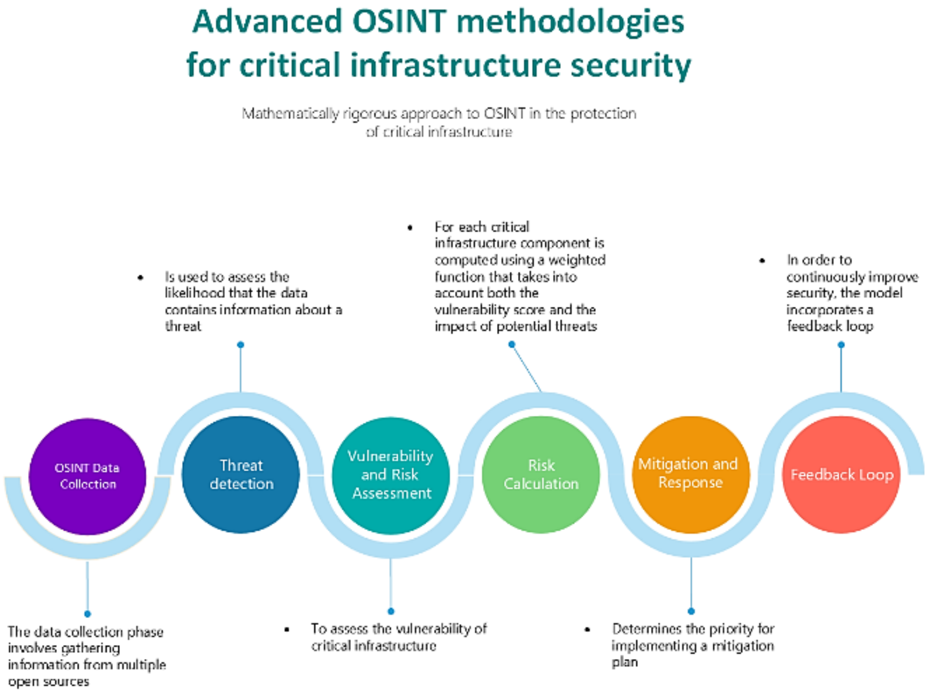
Advanced OSINT methodologies for critical infrastructure security
Mathematically rigorous approach to OSINT in the protection of critical infrastructure
Is used to assess the likelihood that the data contains information about a threat
For each critical infrastructure component is computed using a weighted function that takes into account both the vulnerability score and the impact of potential threats
In order to continuously improve security, the model incorporates a feedback loop
OSINT Data Collection
Threat detection
Vulnerability and Risk Assessment
Risk Calculation
Mitigation and Response
Feedback Loop
The data collection phase involves gathering information from multiple open sources
To assess the vulnerability of critical infrastructure
Determines the priority for implementing a mitigation plan

Fig. 3. Visual presentation of made-up method

These models guide the data collection, threat detection, vulnerability assessment, and risk calculation processes:

Fig. 3: Conventional designations:

- C_1: Set of critical infrastructure components (e.g., power plants, water systems, communications networks).
- S_0: Set of OSINT sources (e.g., social media, government databases, websites, forums).
- D_0: Set of data extracted from OSINT sources.
- V_T: Set of threat vectors identified through OSINT analysis.
- A_l: Set of analysis techniques applied to the OSINT data (e.g., correlation, semantic analysis, geospatial analysis).
- R_s: Risk score calculated based on potential threats and vulnerabilities.
- P_M: Set of mitigation plans or responses.

OSINT Data Collection

The data collection phase involves gathering information from multiple open sources, which are mathematically represented on formula (1):

$$D_0=\{d_1,d_2,...,d_n\}\ where\_d_i\in S_0\,. \tag{1}$$

Each piece of data d_i is associated with a source S_0 and a critical infrastructure component C_1. For example, imagining the situation when data collected about an organization's security policies could be linked to their communication systems.

Threat Detection

For each piece of data d_i, a probability function $P=(T/d_i)$ is used to assess the likelihood that the data contains information about a threat T represented on formula (2):

$$P(T\mid d_i)=\frac{\mathrm{Re}\,levant\_threat-related\_keywords\_found\_in\_d_i}{Total\_data\_po\,\mathrm{int}\,s}. \tag{2}$$

Where $P(T\mid d_i)\in[0,1]$ represents the probability that the data point d_i contains information about a potential threat.

Vulnerability and Risk Assessment

To assess the vulnerability of critical infrastructure, we assign a vulnerability score $V(C_{ij})$ to each component C_{ij}, based on its exposure to open-source threats in the following formula (3):

$$V(C_{ij})=f(D_0,V_t,A_l)\,. \tag{3}$$

This function f considers the data collected D_0, the threat vectors identified V_t, and the analysis techniques applied A_l. For instance, a high volume of OSINT data indicating a cyber threat against a power grid would increase its vulnerability score.

Risk Calculation

Once vulnerabilities have been assessed, the overall risk score $R_s(C_{ij})$ for each critical infrastructure component is computed using a weighted function that takes into account both the vulnerability score and the impact of potential threats showed in formula (4):

$$R_s(C_{ij})=\alpha V(C_{ij})+\beta I(T_j)\,. \tag{4}$$

Where $V(C_{ij})$ is the vulnerability score of the critical infrastructure component, $I(T_j)$ is the impact of the identified threat on that component, α and β are weighting factors based on the likelihood of a threat and the importance of the infrastructure.

Mitigation and Response

The risk score $R_s(C_{ij})$, presented at formula (5), determines the priority for implementing a mitigation plan. The mitigation strategies are represented by a set P_M, which are functions of the risk score:

$$P_M=g(R_s(C_1)). \tag{5}$$

Where g is a decision function that selects appropriate mitigation strategies based on the calculated risk. For example, if $R_s(C_{ij})$ is high, the mitigation plan might involve enhanced monitoring or deploying security patches.

Feedback Loop

In order to continuously improve security, the model incorporates a feedback loop where new data points D_0 and threat vectors V_T are constantly updated, and the risk scores V_T are recalculated:

$$\begin{aligned}D_0^{(t+1)}&=D_0^{(t)}+\Delta D,\\ V_T^{(t+1)}&=V_T^{(t)}+\Delta V,\\ R_S^{(t+1)}&=R_S^{(t)}+\Delta R.\end{aligned} \tag{6}$$

This feedback ensures that the model adapts to new information and evolving threats, keeping the critical infrastructure secure against potential risks.

Results

The study's findings underscore the value of a quantitative OSINT model in critical infrastructure security, demonstrating improvements in accuracy, speed, and decision-making. By reducing ambiguity through probabilistic risk assessments, the model minimizes unnecessary alerts and focuses on actionable threats. Scalability testing showed the model could handle large datasets effectively without overwhelming analysts. Finally, objective risk assessments were validated as enhancing decision-making processes, thus proving beneficial in real-time threat detection and mitigation. The model provides a solid foundation for continuously evolving OSINT practices and suggests potential for further optimization by minimizing risk and balancing mitigation efforts through a defined objective function.

The introduction of a mathematical foundation significantly improves the overall accuracy, efficiency, and reliability of OSINT for critical infrastructure security. Here are the key benefits:

- **Greater Precision**: By assigning probabilities and quantifying risks, our method minimizes the ambiguity inherent in traditional OSINT methods. This allows for more targeted threat mitigation, reducing unnecessary interventions.
- **Enhanced Speed**: Automating the data collection and threat evaluation process using mathematical

formulas accelerates the analysis, enabling faster responses to emerging threats, a crucial factor in protecting critical infrastructure.

- **Scalability**: The structured approach is scalable, capable of processing vast amounts of data across multiple sources without overwhelming analysts. Existing methods struggle to handle large datasets effectively without risking data overload.
- **Objective Decision Making**: Our method removes much of the subjectivity involved in traditional OSINT threat assessments by introducing quantitative models, improving decision-making accuracy for infrastructure protection.

Discussion and conclusions

Also, in conclusion, after all conducted analytical works, we could definitely say that this mathematical model demonstrates how OSINT can be systematically used to enhance the security of critical infrastructure by assessing vulnerabilities, detecting threats, calculating risk, and applying targeted mitigation strategies. It leverages data collection from open sources, threat analysis, and continuous feedback to ensure that infrastructure systems are resilient to evolving risks.

In the metter of optimizing the processes from the persective of mathematical model, we'd recommend the following. The model can be further optimized using an objective function that minimizes risk across all infrastructure components while balancing resource allocation for mitigation in formula 4.1.

Author's contribution: Laryisa Dakova – conceptualization, methodology; Maryana Levytska – analysis of sources, preparation of literature review, theoretical foundations of the study; Katerina Havenko preparation of the laboratory for the study, conducting the study.

References

Best, R. A. Jr. (2011). Open Source Intelligence (OSINT). *Issues for Congress.* Congressional Research Service.

Brown, I. (2010). The changing role of open source intelligence in national security. *Intelligence and National Security*, 25(5), 699–722.

Clarke, R. A. (2011). *Cyber war: The next threat to national security and what to do about it.* HarperCollins Publishers.

Congressional Research Service. (2007, December 5). *Open Source Intelligence (OSINT).* A question for Congress.

Harding, T. (2019). *Open Source Intelligence techniques: Resources for searching and analyzing online information.* CreateSpace Independent Publishing Platform. https://doi.org/10.33896/SPolit.2019.54.11

Johnson, L. (2019). *Artificial intelligence in OSINT. A new frontier for intelligence agencies*. Taylor & Francis Group.

Knight, W. (2020). The impact of social media on intelligence gathering. *Journal of Public Intelligence*, 11(3), 45–56. https://www.researchgate.net/publication/259497232_Social_Media_and_Intelligence_Gathering

Lewis, J. (2021). Geospatial intelligence and OSINT. A convergence of tools and techniques. *Defense & Intelligence Review.*

Lowenthal, M. (2017). *Intelligence: From secrets to policy.* SAGE Publications (7th ed.).

Mutschke, P. (2018). Big data analytics for open source intelligence. New trends and applications. *Journal of Intelligence Studies.* https://ieeexplore.ieee.org/document/8954668

NATO. (2001, November). *NATO Open Source.* Intelligence Handbook.

Schafer, M. (2017). OSINT in the age of social media. *IEEE Access, Cybersecurity Journal*. https://doi.org/10.1109/ACCESS.2020.2965257.

Zegart, A. (2015). *Eyes on spies: Congress and the United States intelligence community.* Hoover Institution Press.

Отримано редакцією журналу / Received: 30.10.24
Прорецензовано / Revised: 27.11.24
Схвалено до друку / Accepted: 30.11.24

Лариса ДАКОВА, канд. техн. наук, доц.
ORCID ID: 0000-0001-6104-8217
e-mail: dacova@ukr.net
Державний університет інформаційно-комунікаційних технологій, Київ, Україна

Мар'яна ЛЕВИЦЬКА, студ.
ORCID ID: 0009-0007-1617-029X
e-mail: levytskam@fit.knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Катерина ГАВЕНКО, студ.
ORCID ID: 0009-0005-7036-9318
e-mail: havenkok@fit.knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

ВИКОРИСТАННЯ ІНТЕЛЕКТУ З ВІДКРИТИМ КОРИСНИМ КОДОМ ДЛЯ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Вступ. ***Критична інфраструктура охоплює системи й активи, необхідні для функціонування сучасного суспільства й економіки. До них належать енергетика, транспорт, телекомунікації, охорона здоров'я та водопостачання – усі ці сектори мають вирішальне значення для національної безпеки та добробуту громадян. Збої в цих інфраструктурах можуть мати серйозні соціально-економічні наслідки.***

З розвитком технологій системи безпеки критичної інфраструктури стають дедалі складнішими та більш взаємопов'язаними. Інновації, такі як інтелектуальні мережі, автоматизовані транспортні системи та складні комунікаційні мережі, не лише підвищують ефективність, але і збільшують вразливість. Конвергенція цифрових і фізичних систем робить вказані сектори чутливішими до ризиків, зокрема і до кібератак, стихійних лих, тероризму й інших загроз. Це підкреслює необхідність для урядів і організацій приділяти особливу увагу захисту цих життєво важливих інфраструктур.

Методи. ***Для захисту критичної інфраструктури розроблено математично точний підхід до використання OSINT (відкритих джерел інформації). Це вдосконалений метод, що включає структуровану модель для виявлення загроз, оцінювання вразливості та розрахунку ризику. Запропонований підхід базується на математичних моделях і ймовірнісних функціях, що дозволяє здійснювати точніший аналіз загроз та оцінювання вразливості. Це дає змогу розробляти ефективніші стратегії пом'якшення наслідків і покращити координацію реагування. На відміну від традиційних методів OSINT, які покладаються на збір і аналіз неструктурованих даних, наш підхід запроваджує математичну основу для збору даних і оцінювання загроз, забезпечуючи вдосконалене представлення даних і ймовірнісне виявлення загроз.***

Результати. ***Результати дослідження підтверджують ефективність кількісної моделі OSINT для безпеки критичної інфраструктури. Вона демонструє поліпшення точності, швидкості прийняття рішень, мінімізуючи невизначеність завдяки ймовірнісному оцінюванню ризиків. Модель зменшує кількість непотрібних сповіщень і фокусується на загрозах, що мають практичне значення. Тестування на масштабованість показало, що система здатна ефективно обробляти великі обсяги даних, не перевантажуючи аналітиків. Об'єктивні оцінки ризиків підтвердили поліпшення процесу прийняття рішень і допомогли виявляти і пом'якшувати загрози в реальному часі. Модель також дає надійну основу для подальшого розвитку практик OSINT, з можливістю подальшої оптимізації через зменшення ризиків і збалансування зусиль щодо їхньої нейтралізації.***

Висновки. ***Результати дослідження показують, що запропонована математична модель є ефективним інструментом для систематичного застосування OSINT для підвищення безпеки критичної інфраструктури. Вона дозволяє здійснювати оцінювання вразливостей, виявлення загроз, розрахунок ризику та застосовувати цілеспрямовані стратегії пом'якшення. Завдяки використанню відкритих джерел даних, аналізу загроз і постійному зворотному зв'язку, модель забезпечує стійкість інфраструктури до мінливих ризиків.***

Ключові слова: ***OSINT, безпека критичної інфраструктури, кіберзагрози, оцінка вразливості, стійкість інфраструктури, публічні джерела, аналіз даних, кібербезпека, інформаційна безпека.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.