Decision-making process model for cybersecurity protection of critical infrastructure objects under the hybrid threats influence

Модель процесу прийняття рішень щодо захисту кібербезпеки об'єктів критичної інфраструктури під впливом гібридних загроз

Volodymyr Shypovskyi * [A]

* **Corresponding author**: PhD student, e-mail: stratcom.ndl@gmail.com, ORCID: 0000-0003-3743-3064

[A] National Defense University of Ukraine, Kyiv, Ukraine

Володимир Шиповський * [A]

* **Corresponding author**: Ад'юнкт кафедри, e-mail: stratcom.ndl@gmail.com, ORCID: 0000-0003-3743-3064

[A] Національний університет оборони України, м. Київ, Україна

Received: May 30, 2023 | Revised: June 26, 2023 | Accepted: June 30, 2023

DOI: 10.33445/sds.2023.13.3.3

Purpose: is to develop a model and mathematical framework for the decision-making process regarding the cybersecurity of information systems of critical infrastructure objects, taking into account the properties and requirements of objects that have strategic importance for the state.

Method: is based on a comprehensive approach that combines analysis of contemporary information sources, expertise, and analytical data from leading cybersecurity professionals, as well as linear mathematical modeling.

Theoretical implications: include proposing an adapted decision-making model for protecting critical infrastructure from hybrid threats by integrating frameworks and emphasizing adaptability, it enhances the understanding of decision-making processes in cybersecurity.

Practical consequences. It represents an innovative decision-making model aimed at protecting critical infrastructure and enabling rapid response to cyber threats. It combines the frameworks of existing models, the OODA (Observe, Orient, Decide, Act) loop and PDCR (Plan, Do, Check, React), widely applied in cybersecurity across various industries. This adaptive model allows for observation, analysis, and response to emerging cyber risks, ensuring the necessary level of cyber resilience. The developed model provides a practical tool for safeguarding critical infrastructure and minimizing damage in a growing threat landscape

Paper type: theoretical.

Мета роботи: є розробка моделі та математичного апарату для процесу прийняття рішення щодо кіберзахисту інформаційних систем об'єктів критичної інфраструктури, враховуючі властивості та вимоги об'єктів, які мають стратегічно-важливе значення для держави.

Метод дослідження: комплексний підхід, що поєднує аналіз сучасних інформаційних джерел, досвід та аналітичні дані провідних фахівців галузі кібербезпеки та лінійне математичне моделювання.

Теоретична цінність дослідження: включають пропозицію адаптованої моделі процесу прийняття рішень для захисту критичної інфраструктури від гібридних загроз шляхом інтеграції рамок і наголошування на адаптивності, вона покращує розуміння процесів прийняття рішень у кібербезпеці.

Практична цінність дослідження: являє собою новаторську модель процесу прийняття рішень, спрямовану на захист критичної інфраструктури та швидке реагування на загрози у кіберпросторі. Вона поєднує рамки існуючих моделей OODA loop та PDCR, які широко застосовуються для кіберзахисту інформаційної інфраструктури в багатьох виробничих галузях. Ця адаптивна модель дозволяє спостерігати, аналізувати та реагувати на нові кіберризики, забезпечуючи необхідний рівень кіберстійкості системи. Розроблена модель надає практичний інструмент для захисту критичної інфраструктури та зменшення шкоди в зростаючому загрозливому середовищі.

Тип статті: теоретична.

Key words: cyberresilience, critical infrastructure, model, information security.

Ключові слова: кіберстійкість, критична інфраструктура, модель, безпека інформації.

1. Introduction

Critical infrastructure systems are essential for providing basic necessities such as energy, transportation, and healthcare services. However, cyber attacks have emerged as a significant threat to their security and stability. Although this problem has been widely researched, there is still a need for more comprehensive and integrated approaches to address it. This study aims to develop a logical model for implementing cyber attacks on critical infrastructure systems and evaluating their security posture against these attacks. The research tasks include analyzing the existing literature, identifying critical components, evaluating security posture, and proposing effective mitigation strategies. The scientific novelty of this research lies in the development of a logical model for implementing cyber

attacks on critical infrastructure systems. The practical significance is providing a framework for security analysts and system administrators to assess security posture and develop effective mitigation strategies against cyber threats.

2. Data and methods

In this research, a comparative analysis of two popular cyber defense models, namely PDCA (Plan-Do-Check-Act) and OODA (Observe-Orient-Decide-Act) Loop, and proposed a new decision-making process model for cyber defense of critical assets infrastructure. During the comparative analysis, we determined the advantages and disadvantages of both models in the context of cyber attacks on critical infrastructure and identified limitations that require attention. Based on the analysis, using mathematical modeling and theory of algorithms, a new logical model was developed, which uses the advantages of both the PDCA model and the OODA Loop model, taking into account their limitations, and developed a mathematical apparatus that takes into account the features of information systems of critical infrastructure objects in conditions of hybrid threats.

3. Theoretical background

There are several popular methods and models for cyberprotection of critical infrastructure, including the Defense-in-Depth (DiD) approach (Election Security Spotlight – Defense in Depth, 2022), Risk Management Framework (RMF) (Risk Management Framework, 2018), and the Cyber Kill Chain (CKC) model (The Cyber Kill Chain Explained, 2015). The DiD approach is based on the idea of layering multiple security measures to protect critical infrastructure systems from cyber threats. This approach involves the use of multiple layers of security controls, such as firewalls, intrusion detection systems, and access controls, to create a series of barriers against cyber attacks. The DiD approach is widely adopted in the cybersecurity industry, and several guidelines and standards, such as NIST SP 800-53 and ISO/IEC 27001, recommend its use. The RMF approach is a structured, repeatable process for managing the risks associated with an organization's information systems. This approach is based on the principles of the NIST SP 800-37 publication and is designed to help organizations identify, assess, and prioritize risks to their information systems. The CKC model is a military-inspired approach to cybersecurity that focuses on the various stages of a cyber attack, from initial reconnaissance to final exfiltration of data. This approach involves the use of several defensive measures to detect and respond to attacks at different stages of the attack lifecycle.

While these methods and models have their strengths, the PDCA and OODA Loop models are particularly suitable for critical infrastructure cybersecurity. The PDCA model (What is the plan-do-check-act cycle? 2018) involves a continuous cycle of planning, implementing, monitoring, and adjusting security measures to ensure their effectiveness. This model is well-suited for critical infrastructure cybersecurity because it emphasizes the need for continuous improvement and adaptation to changing threats. Similarly, the OODA Loop model emphasizes the importance of rapid decision-making and adaptation in response to changing threat environments. This model involves a continuous cycle of observing the environment, orienting oneself to the situation, making a decision, and taking action. The OODA Loop model is particularly relevant for critical infrastructure cybersecurity because it emphasizes the need for rapid decision-making and response to mitigate the impact of cyber attacks. Overall, while there are several methods and models for cyber protection of critical infrastructure, the PDCA and OODA Loop models are particularly relevant for their emphasis on continuous improvement, adaptation, and rapid response to changing threat environments.

4. Results

Overall, the OODA Loop and PDCA models are both useful approaches for improving cybersecurity in critical infrastructure. The OODA Loop model emphasizes the importance of rapid decision-making and adaptation in response to changing threat environments. This model involves a continuous cycle of observing the environment, orienting oneself to the situation, making a decision, and taking action. The OODA Loop model is particularly relevant for critical infrastructure cybersecurity because it emphasizes the need for rapid decision-making and response to mitigate the impact of cyber attacks. On the other hand, the PDCA model involves a continuous cycle of planning, implementing, monitoring, and adjusting security measures to ensure their effectiveness. This model is well-suited for critical infrastructure cybersecurity because it emphasizes the need for continuous improvement and adaptation to changing threats. Both models share a focus on continuous improvement and adaptation, but differ in their emphasis on rapid decision-making versus continuous monitoring and adjustment. In critical infrastructure cybersecurity, it is important to have a balance between these two approaches, as rapid decision-making is necessary in response to cyber attacks, but continuous monitoring and adjustment is needed to ensure the effectiveness of security measures over time.

Both the OODA Loop and PDCA models have their strengths and weaknesses, but when used in combination, they can provide a comprehensive and effective approach to cybersecurity in critical infrastructure. By continually assessing and improving security measures, organizations can better protect their critical infrastructure systems from cyber threats.

The OODA Loop Model is a decision-making framework developed by military strategist and United States Air Force Colonel John Boyd. It consists of four iterative stages: Observe, Orient, Decide, and Act. The first stage, "Observe", involves gathering information about the environment and potential threats. This includes monitoring network activity, analyzing data, and identifying potential vulnerabilities. The second stage, "Orient", involves interpreting and analyzing the information collected during the observation phase. This includes evaluating the threat level, assessing the impact of an attack, and understanding the capabilities and motivations of the attacker. The third stage, "Decide", involves making informed decisions about how to respond to the threat. This includes developing a plan of action, determining the appropriate level of response, and identifying potential risks and consequences. The fourth and final stage, "Act", involves implementing the plan of action and responding to the threat. This includes deploying defensive measures, investigating the attack, and restoring systems to their normal state. The OODA Loop Model emphasizes the importance of speed and agility in responding to threats. By continually iterating through the four stages, organizations can quickly detect and respond to cyber attacks, reducing the risk of data loss, system downtime, and reputational damage.

The OODA Loop Model is a decision-making process that involves four main stages: Observe, Orient, Decide, and Act. Here is a general algorithm for the OODA Loop Model:

Observe: Collect data and information about the current situation.

a. Identify relevant sources of information.

b. Monitor changes in the environment or situation.

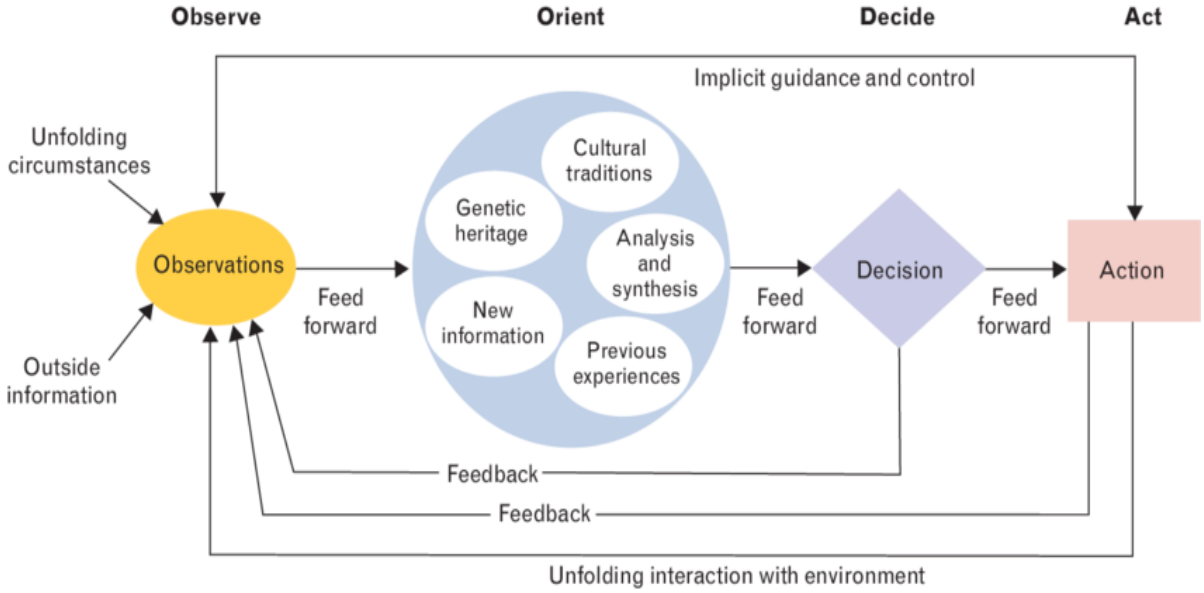
c. Analyze the data and information collected.

Orient: Analyze and interpret the data and information to gain understanding of the situation.

a. Evaluate the current situation.

b. Assess the potential risks and threats.

c. Identify any biases or assumptions that may affect the interpretation of the data.



Picture 1 – OODA loop

Decide: Develop and select a course of action based on the analysis and interpretation of the data.

a. Generate possible courses of action.

b. Evaluate the potential outcomes of each course of action.

c. Select the most appropriate course of action based on the analysis.

Act: Implement the selected course of action.

Figure 1 – OODA loop

a. Communicate the decision and the course of action to relevant parties.

b. Implement the plan.

c. Monitor the results and adjust the plan if necessary.

In terms of logical formulas, the OODA Loop Model involves a series of if-then statements, where the decision-making process is based on the results of each stage. For example:

If observation reveals a potential threat, then orientation involves assessing the severity of the threat and identifying any vulnerabilities in the system.

If the analysis of the data indicates a need for action, then the decision stage involves selecting the most appropriate course of action based on the analysis.

If the selected course of action does not produce the desired results, then the action stage involves monitoring the results and adjusting the plan if necessary.

The OODA Loop Model can be mathematically described using the following formulas:

Observe (O): In this step, information is collected and processed from various sources. This can be represented by the following formula:

$$O = f(i1, i2, i3, ..., ir) \quad (1)$$

where *O* represents the observed information, and *i1*, *i2*, *i3*, ..., *ir* – represent the different sources of information.

Orient (O'): In this step, the observed information is analyzed and interpreted to understand the current situation. This can be represented by the following formula:

$$O' = f(O, c1, c2, c3, ..., cm) \quad (2)$$

where *O'* represents the orientation, and c1, c2, c3, ..., cm represents the different factors that affect the orientation process.

Decide (D): In this step, a decision is made based on the orientation. This can be represented by the following formula:

$$D = f(O', m1, m2, m3, ..., mp) \quad (3)$$

where *D* represents the decision, and m*1*, m*2*, m*3*, ..., mp represent the different options or alternatives available.

Act (A): In this step, the decision is implemented. This can be represented by the following formula:

$$A = f(D, e1, e2, e3, ..., en) \quad (4)$$

where A represents the action, and e*1*, e*2*, e*3*, ..., e*n* represent the different resources or methods used to implement the decision.

The OODA Loop Model is a continuous process, and after the action step, the cycle repeats itself by going back to the observe step.

In the context of cyber protection, the PDCA model is a popular approach for continuously improving an organization's cybersecurity posture. The model consists of four steps: *Plan, Do, Check,* and *Act.*

The *Plan phase* involves identifying the risks and threats to the organization's critical infrastructure systems, and developing a plan to mitigate those risks. This includes defining security policies, procedures, and guidelines, as well as identifying the resources and tools necessary for implementing those measures.

The *Do phase* involves implementing the security measures identified in the Plan phase. This includes training employees on security best practices, implementing security technologies such as firewalls and intrusion detection systems, and regularly updating and patching software and hardware.

The *Check phase* involves monitoring the effectiveness of the security measures implemented in the Do phase. This includes conducting regular security assessments, vulnerability scans, and penetration testing to identify any gaps or weaknesses in the organization's security posture.

The *Act phase* involves taking action based on the results of the Check phase. This includes making any necessary adjustments to the security measures implemented in the Do phase to improve their effectiveness, as well as updating the security plan to address any new risks or threats.

The ***PDCA model*** (The Importance of the PDCA Cycle) provides a structured approach for organizations to continuously improve their cybersecurity posture. By regularly assessing and adjusting their security measures, organizations can better protect their critical infrastructure systems from cyber threats. The model emphasizes the importance of a proactive approach to

cybersecurity, as well as the need for ongoing monitoring and adjustment to ensure the effectiveness of security measures over time.

In the context of cyber protection, the PDCA model is a popular and effective approach for managing cybersecurity risks and protecting critical infrastructure systems. The model emphasizes the importance of a continuous cycle of improvement, which involves identifying potential risks and vulnerabilities, implementing security measures to mitigate those risks, monitoring the effectiveness of those measures, and making adjustments to improve their effectiveness over time.

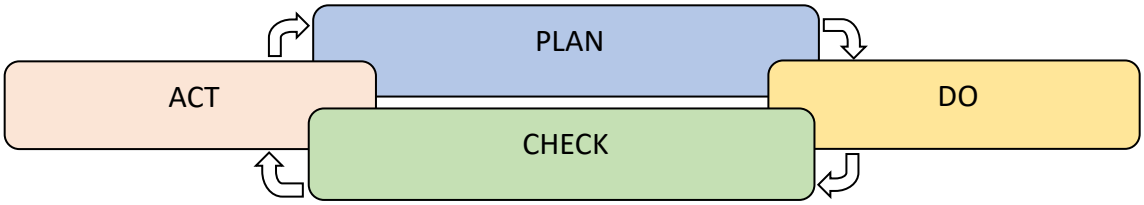


Figure 2 – PDCA model

The PDCA model also emphasizes the importance of a proactive approach to cybersecurity, which involves regularly assessing the organization's security posture and making necessary adjustments to mitigate emerging threats. By adopting a continuous improvement mindset, organizations can stay ahead of cyber threats and protect their critical infrastructure systems from potential attacks.

One of the key benefits of the PDCA model is that it provides a structured and systematic approach to managing cybersecurity risks. This approach enables organizations to identify and prioritize risks, allocate resources effectively, and implement security measures in a strategic and efficient manner.

Moreover, the PDCA model is a flexible framework that can be adapted to different organizations and industries. This allows organizations to tailor their cybersecurity measures to their specific needs and risks.

Overall, the PDCA model is a valuable tool for managing cybersecurity risks in critical infrastructure systems. Its emphasis on continuous improvement, proactive risk management, and systematic implementation of security measures makes it an effective approach for protecting against emerging cyber threats.

The PDCA (Plan-Do-Check-Act) model can be represented mathematically as follows:

Plan: During this phase, the organization identifies potential risks and vulnerabilities and develops a plan to mitigate those risks. This can be represented mathematically as:

$$P = f(RV, M, S) \tag{5}$$

where P represents the plan, RV represents the identified risks and vulnerabilities, M represents the organization's resources, and S represents the desired security measures.

Do: In this phase, the organization implements the plan by putting security measures in place. This can be represented mathematically as:

$$D = f(P, Ism) \tag{6}$$

where D – represents the implementation of the plan, P represents the plan, and Ism – implemented security measures.

Check: During this phase, the organization evaluates the effectiveness of the implemented security measures by monitoring their performance. This can be represented mathematically as:

$$C = f(Ism, KPI) \quad (7)$$

where C represents the evaluation of the implemented security measures, IM represents the implemented security measures, and *KPI* represents the key performance indicators used to measure their effectiveness.

Act: Based on the results of the evaluation, the organization takes action to improve the effectiveness of the security measures. This can be represented mathematically as:

$$A = f(C, Ir) \quad (8)$$

where *A* – action taken to improve the security measures;

C – evaluation of the implemented security measures;

Ir – the recommended improvements.

The *table 1* presents the general advantages and disadvantages of both models. But the purpose of the research is to select (improve) a model for information systems of critical infrastructure objects that have certain differences and requirements.

Table 1 – Advantages and disadvantages of models

Model	Advantages	Disadvantages
PDCA	- Emphasizes planning and prevention; - Systematic approach to problem solving; - Focuses on continuous improvement and adaptation; - Applicable in various fields beyond cyber protection.	- Can be time-consuming and resource-intensive; - May not be suitable for rapidly changing environments; - Can be difficult to implement without strong organizational support and commitment.
OODA Loop	- Emphasizes speed and agility; - Encourages experimentation and adaptation; - Can be effective in rapidly changing environments; - Allows for rapid response to emerging threats.	- May not emphasize enough on planning and prevention; - Can be prone to errors in decision making; - Can be difficult to implement without strong leadership and clear communication.

Information systems of critical infrastructure objects have more stringent cybersecurity requirements compared to other types of information systems. Some of the key differences and requirements for information systems of critical infrastructure objects in cybersecurity aspects are:

Differences:

Criticality: Information systems of critical infrastructure objects are more critical than other types of information systems. As a result, a cybersecurity breach or attack on these systems can cause significant damage and have severe consequences.

Complexity: Information systems of critical infrastructure objects are more complex than other types of information systems. They are interconnected with other systems and handle large volumes of data in real-time.

Threat landscape: Information systems of critical infrastructure objects are more likely to face advanced and persistent cyber threats than other types of information systems.

Requirements:

Risk assessment: Information systems of critical infrastructure objects require a comprehensive risk assessment to identify and prioritize potential cyber threats.

Access control: Access control measures, such as multi-factor authentication, must be implemented to ensure that only authorized personnel can access critical information systems.

Continuous monitoring: Information systems of critical infrastructure objects require continuous monitoring to detect and respond to cybersecurity incidents in real-time.

Incident response planning: Information systems of critical infrastructure objects require a well-defined incident response plan to ensure that any cybersecurity incidents are handled in a timely and effective manner.

Security testing: Regular security testing, including vulnerability assessments and penetration testing, is necessary to identify and address potential vulnerabilities in the information systems.

Compliance: Information systems of critical infrastructure objects must comply with relevant cybersecurity regulations and standards, such as NIST Cybersecurity Framework, IEC 62443, and ISO 27001.

Collaboration and communication: Effective collaboration and communication between IT, security, and operations teams are necessary to ensure the effective implementation of cybersecurity measures.

Information systems of critical infrastructure objects require more stringent cybersecurity measures due to their criticality, complexity, and the advanced cyber threats they face (The System of Cybersecurity). Comprehensive risk assessment, access control, continuous monitoring, incident response planning, security testing, compliance, and collaboration and communication are crucial for ensuring the cybersecurity of information systems of critical infrastructure objects.

Table 2 describes the limits of model OODA Loop and PDCA for analysis and selection of a model more suitable for critical infrastructure objects.

Table 2 – Models limitations

Model	Limitations
PDCA	- Can be time-consuming and resource-intensive; - May not be suitable for rapidly changing environments; - Can be difficult to implement without strong organizational support and commitment; - May not be suitable for addressing complex and adaptive threats.
OODA Loop	- May not emphasize enough on planning and prevention; - Can be prone to errors in decision making; - Can be difficult to implement without strong leadership and clear communication; - May not be suitable for addressing long-term and strategic threats.

It's important to note that these limitations should not discourage organizations from using these models. Instead, organizations should carefully consider these limitations and adapt the models to their specific needs and contexts in order to maximize their effectiveness in cyber protection.

Based on the advantages and disadvantages of the models considered in the study, taking into account the limitations of the models and the requirements for information systems of critical infrastructure objects, the proposed model ITASA is presented in *figure 3*.

A feature of the proposed model is the consideration of the most important requirements for information systems of critical infrastructure objects – namely, *time* and *adequate response* of the system (operator) to threats. The model consists of three main component blocks: ***inspection, threat assessment*** and ***system adjustment***. The ITASA Model as OODA Loop Model is a continuous

process, and after the *system adjustment* step, the cycle repeats itself by going back to the *inspection* step.

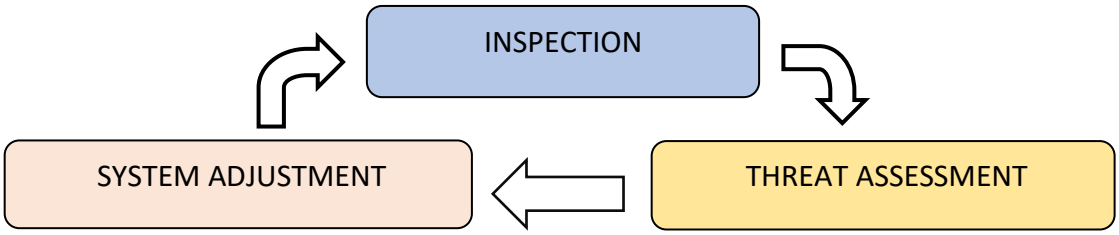


Figure 3 – ITASA model

The logical model of ITASA is presented in the form of an algorithm that shows the following sequence of events:

block No. 1: Evaluation of the system in terms of internal and external threats;

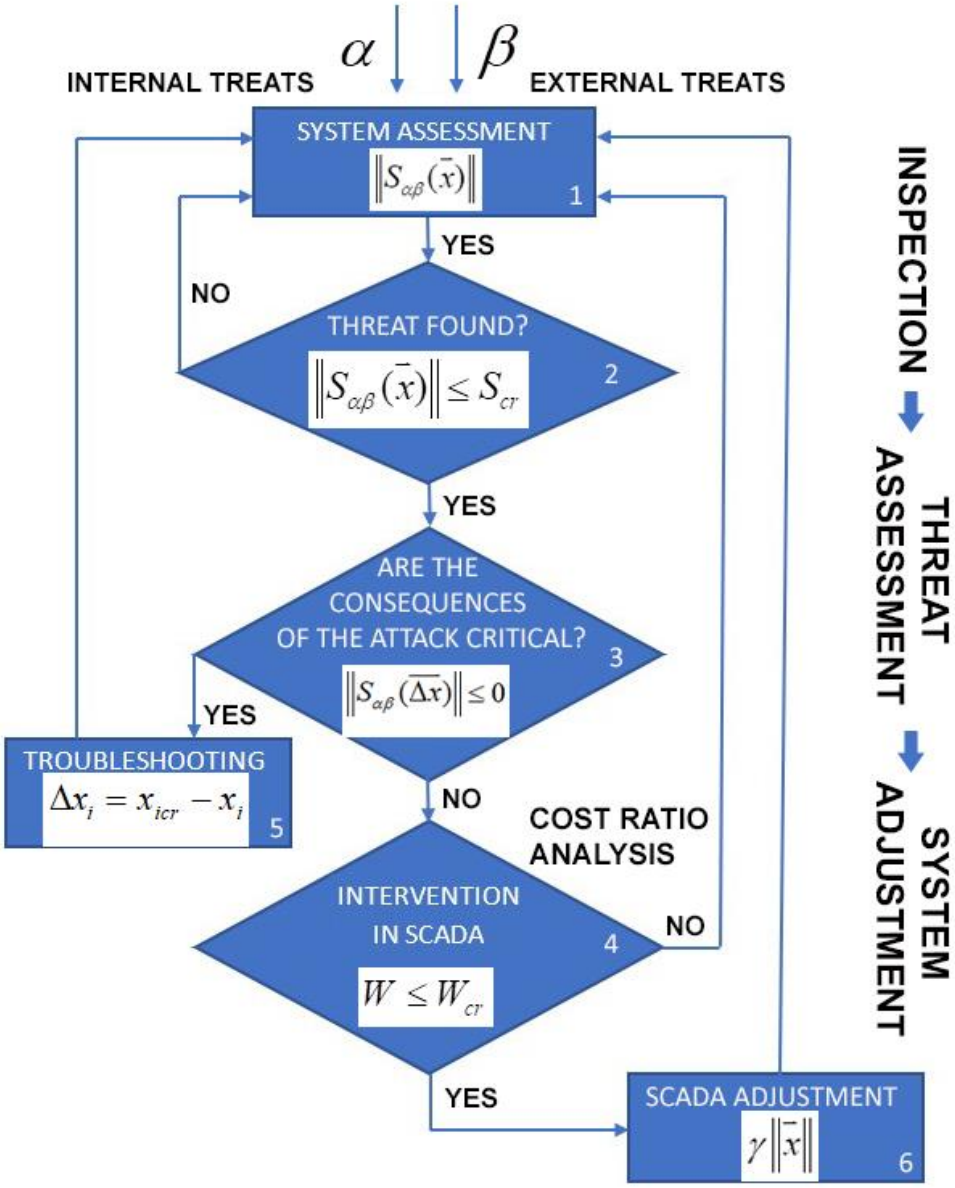


Figure 4 – Logical ITASA model

block No.2: Detection of destructive influence on information processes in the system;

unit No.3: Assessment of the criticality of the consequences of a cyberattack.

block No.4: Assessment of possible changes in the operation of the SCADA system of the critical infrastructure object;

block No.5: Troubleshooting

block No. 6: Adaptation of the operation of the SCADA system to the existing conditions.

To formalize the mentioned approach, consider the system $S_{\alpha\beta}(\vec{x})$, which is described by the vector of parameters $\vec{x} = (x_1, x_2, \dots x_n)$ which is subjected to external destructive influences – α, or internal destructive influences – β, then mathematically these influences can be represented:

$$\overrightarrow{x_\alpha} = (x_{1\alpha}, x_{2\alpha}, \dots, x_{n\alpha}), \quad (9)$$

$$\overrightarrow{x_\beta} = (x_{1\beta}, x_{2\beta}, \dots, x_{n\beta}), \quad (10)$$

$$S_{\alpha\beta}(\vec{x}) = S(\vec{x} + \overrightarrow{x_\alpha} + \vec{x}_\beta), \quad (11)$$

Then the evaluation of the system can be carried out as follows (block #2):

$$\left\|S_{\alpha\beta}(\vec{x})\right\| = \sqrt{{x_1}^2 + {x_2}^2 + \dots + x_n^2}, \quad (12)$$

$$\left\|S_{\alpha\beta}(\vec{x})\right\| \le S_{cr}, \quad (13)$$

In this expression: S_{cr} – a system value that is critical to the information system of a critical infrastructure facility. If the conditions of formula (13) are not met, then we proceed to block №4:

$$\Delta x_i = {x_i}_{cr} - x_i, \quad (14)$$

$$\left\|S_{\alpha\beta}(\overrightarrow{\Delta x})\right\| \le 0, \quad (15)$$

If the conditions of expression (15) are satisfied, we proceed to block №5, if not, we compare the losses of the critical infrastructure object:

$$W = \sqrt{\sum_{i=1}^{k} \gamma_i {x^2}_{\alpha\beta_i}}, \quad (16)$$

$$W = W_{cr}, \quad (17)$$

In this formula:

W – losses in case of partial failure of critical infrastructure facilities;

Wcr – losses in case of complete cessation of operation of the critical infrastructure object;

γ_i – the weight factor of the *i*-th measure to restore the functioning of the system.

Block №6 shows the process of adapting the system to the current conditions until the moment of complete elimination of the consequences of the cyber attack and the functioning of the system.

5. Conclusion

The article presents a comprehensive model of the decision-making process for ensuring cybersecurity protection of critical infrastructure objects under the influence of hybrid threats. The model takes into account all the key characteristics of critical infrastructure objects, including time,

complexity of architecture, strategic importance, systematicity, and distribution. The research highlights the importance of addressing the unique challenges posed by hybrid threats, which combine elements of both traditional and cyber warfare. By considering the impact of hybrid threats, the model offers a comprehensive approach to cybersecurity, ensuring the stability and continuity of critical infrastructure operations. The development of the proposed model involved a meticulous analysis of the specific characteristics and requirements of critical infrastructure objects, where time is a crucial factor in effectively responding to cyber threats. The model emphasizes the need for rapid detection, containment, and recovery of critical infrastructure objects to minimize potential damage from cyber attacks.

Additionally, we have taken into account the increased complexity of infrastructure architecture in our decision-making process. This complexity requires a flexible and adaptive approach that can address the dynamic and evolving nature of cyber threats. Real-time monitoring, threat understanding, and continuous improvement processes are integral components of our model, providing active defense against emerging cyber risks. Furthermore, was recognized the strategic importance of critical infrastructure objects and prioritize risk management accordingly. During the model development, the systematicity and distribution of critical infrastructure objects were also considered.

Therefore, the ITASA model presented in the article offers a comprehensive and adaptable approach to cybersecurity for critical infrastructure objects. By considering the unique characteristics and challenges of such objects, including time, complexity of architecture, strategic importance, systematicity, and distribution, our model provides a robust framework for decision-making in the face of hybrid threats.

Recommendations

Based on the findings of this scientific article, the following recommendations are proposed for the application and further development of the model of the decision-making process for cybersecurity protection of critical infrastructure objects under the influence of hybrid threats:

Adoption of the Model: Organizations responsible for the cybersecurity protection of critical infrastructure should consider adopting the proposed model as a framework for decision-making. The model's comprehensive approach, specifically designed to address hybrid threats, makes it especially useful in these challenging conditions.

Integration of Real-time Monitoring: Organizations should prioritize the integration of real-time monitoring capabilities into their cybersecurity systems. This ensures prompt detection of cyber threats and enables quick response and mitigation actions, reducing the potential impact of attacks.

Continuous Improvement: The model emphasizes the importance of a continuous improvement process. Organizations should establish mechanisms to regularly update and enhance their cybersecurity measures, taking into account emerging cyber threats and evolving technologies. Continuous learning and adaptation are essential to effectively counter hybrid threats.

Collaboration and Information Sharing: Organizations should foster collaboration and information sharing among relevant stakeholders involved in the protection of critical infrastructure. This includes sharing threat intelligence, best practices, and lessons learned. Establishing partnerships and communication channels between public and private sectors, as well as across different critical infrastructure sectors, can significantly enhance the overall cybersecurity resilience.

Regular Risk Assessments: Conducting regular risk assessments specific to hybrid threats is crucial. Organizations should identify and assess potential vulnerabilities and risks posed by the convergence of physical and cyber threats. These assessments should inform the development and implementation of appropriate cybersecurity measures, considering the unique characteristics of hybrid threats.

Training and Awareness: Organizations should invest in cybersecurity training and awareness programs for their personnel. Training should cover the identification and response to hybrid threats, emphasizing the need for a proactive and collaborative approach. Raising awareness about the evolving threat landscape and the importance of cybersecurity among all stakeholders is essential for effective protection.

Regulatory and Policy Support: Policymakers and regulators should consider incorporating the principles and recommendations of the model into relevant cybersecurity regulations and policies. This will provide a standardized framework for critical infrastructure protection, ensuring consistency and effectiveness across different organizations and sectors.

In conclusion, the model of the decision-making process for cybersecurity protection of critical infrastructure objects under the influence of hybrid threats presented in this article offers valuable insights and recommendations for organizations. Implementing this model, along with the suggested recommendations, can enhance cybersecurity resilience and enable effective protection against the complex challenges posed by hybrid threats.

6. Funding

This study received no specific financial support.

7. Competing interests

The authors declare that they have no competing interests.

References

1. Election Security Spotlight – Defense in Depth (DiD). (2022). Retrieved from https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-defense-in-depth-did
2. Risk Management Framework (RMF). (2018). Available from : https://www.techtarget.com/searchcio/definition/Risk-Management-Framework-RMF
3. The Cyber Kill Chain (CKC) Explained. (2015). Available from : https://heimdalsecurity.com/blog/cyber-kill-chain-model/
4. What is the plan-do-check-act (PDCA) cycle? (2018). Available from : https://asq.org/quality-resources/pdca-cycle
5. How to use the OODA loop to improve network security. (2021). Available from : https://www.techtarget.com/searchsecurity/tip/How-to-use-the-OODA-loop-to-improve-network-security

Список використаних джерел

1. Election Security Spotlight – Defense in Depth (DiD). (2022). Retrieved from https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-defense-in-depth-did
2. Risk Management Framework (RMF). (2018). Available from : https://www.techtarget.com/searchcio/definition/Risk-Management-Framework-RMF
3. The Cyber Kill Chain (CKC) Explained. (2015). Available from: https://heimdalsecurity.com/blog/cyber-kill-chain-model/
4. What is the plan-do-check-act (PDCA) cycle? (2018). Available from : https://asq.org/quality-resources/pdca-cycle
5. How to use the OODA loop to improve network security. (2021). Available from : https://www.techtarget.com/searchsecurity/tip/How-to-use-the-OODA-loop-to-improve-network-security

6. Integrated Sensing and Decision Support. Kenneth Senne, Gary Condon. (2007). Available from : https://www.researchgate.net/publication/270218307_Integrated_Sensing_and_Decision_Support
7. The Importance of the PDCA Cycle in Driving Continuous Improvement in Organizations. Qualityze. (2013) Available from : https://www.qualityze.com/pdca-cycle-for-continuous-improvement-in-organizations/
8. The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments. Lev Streltsov. European Journal for Security Research. (2017). Available from : https://heimdalsecurity.com/blog/cyber-kill-chain-model/

6. Integrated Sensing and Decision Support. Kenneth Senne, Gary Condon. (2007). Available from : https://www.researchgate.net/publication/270218307_Integrated_Sensing_and_Decision_Support
7. The Importance of the PDCA Cycle in Driving Continuous Improvement in Organizations. Qualityze. (2013) Available from : https://www.qualityze.com/pdca-cycle-for-continuous-improvement-in-organizations/
8. The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments. Lev Streltsov. European Journal for Security Research. (2017). Available from : https://heimdalsecurity.com/blog/cyber-kill-chain-model/