SOCIO-CYBER-PHYSICAL SYSTEMS' THREATS CLASSIFIER

Stanislav Milevskyi
Corresponding author
Department of Cybersecurity[1]
milevskiysv@gmail.com

Oleksandr Korchenko
Department of Information Systems&Technologies Security Academic University of the National Education Commission
2 Podchorążych str., Cracow, Poland, 30-084

Serhii Yevseiev
Department of Cybersecurity[1]

[1]*National Technical University "Kharkiv Polytechnic Institute"*
2 Kyrpychova str., Kharkiv, Ukraine, 61002

Summary: The article considers a new approach to the formation of a threat classifier in socio-cyber-physical systems. These systems, as a rule, are complex and based on the synthesis of cyber-physical components using smart technologies and social networks. It is important to note that these systems also belong to critical infrastructure objects, which requires a new approach to the creation of multi-contour security systems. An important task for the formation of the security contour of such systems is the development of a threat classifier that allows to objectively assess the criticality of the organization's infrastructure elements. The presented classifier allows to define an expert approach at the initial stage for establishing weighting factors of the influence of threats, such as anomalies, deviations from normal functioning and computer incidents. At the next stage, the characteristics of the impact of threats on the platforms of socio-cyber-physical systems, as well as their impact on the external and internal aspects of the system, are determined. The influence of social engineering methods, which can significantly increase the risk of threat implementation and create various channels for their implementation, including mixed (targeted) attacks, is considered in detail. On the basis of the proposed approach to the classification of threats, a method of assessing the current state of the level of security of socio-cyber-physical systems and the possibilities of determining the critical points of the system infrastructure is proposed. Countermeasures and the ability of multi-loop security systems to provide effective infrastructure protection are also discussed.

Keywords: socio-cyber-physical systems, information security, cyber security, information threat classifier of socio-cyber-physical systems, multi-contour information security system.

1. Introduction

The modern development of technologies and computing capabilities contributes to the evolutionary movement towards the creation of integrated systems based on the combination of various technologies, such as the Internet, the Internet of Things, mobile technologies, social systems and networks [1–5]. These systems form socio-cyber-physical systems that allow to obtain emergent properties based on the combination of mesh networks with wireless communication channels and smart technologies. As a result, hybrid systems appear, which usually belong to critical infrastructure objects and attract the attention of attackers.

The emergence of decentralized systems and networks based on blockchain technology makes countering mixed (targeted) attacks on the infrastructure of socio-cyber-physical systems even more difficult [6–10]. In such systems, the physical platform includes sensors, and controls, often located in the cloud, while the social platform includes social networks and messengers. An important task for the formation of the security contour of such systems is the development of a threat classifier that allows to objectively assess the criticality of the organization's infrastructure elements and take into account the criticality of information resources, such as the level of security. This approach makes it possible to consider information resources as a commodity and to form appropriate models for minimizing both hacking risks and financial losses.

The examination of trends in the evolution of mixed threats, particularly targeted attacks, reveals an active "cloning" of the threat vector driven by the increasing demand for digitized services. This evolution is closely tied to the ongoing advancement of computing equipment and technologies. Notably, the advent of socio-cyber-physical systems and the proliferation of diverse digital services, alongside the development of full-scale quantum computers, holds significant importance.

Existing research [1–5] provides various frameworks for the classification of threats. However, these approaches overlook the possibility of categorizing threats into distinct security components, such as cyber security (CS), information security (IS), and security of information (SI). Furthermore, they fail to consider the nuanced impact of these threats on vital aspects of security services, including but not limited to confidentiality, integrity, authenticity, availability, and participation.

The study [8] introduces a synergistic approach to constructing a threat model; however, it overlooks the potential impact of social engineering methods, which can significantly enhance the execution of targeted (mixed) threats. On the other hand, the work [11] addresses a general approach to universalizing classifier construction but fails to acknowledge the necessity of developing multi-circuit information protection systems in the context of operating multi-platform systems, which encompass cyber-physical systems.

Therefore, the analysis underscores that, amid the evolutionary growth of hybrid (complex) systems amalgamating various technologies, a critical focus should be on establishing multi-circuit protection systems that account for defined platforms. It's equally crucial to consider the repercussions of threats on both external and internal security circuits.

The primary objective of this article is to formulate a threat classifier tailored for socio-cyber-physical systems. This classifier takes into consideration the hybridity and synergy inherent in targeted (mixed) attacks, the integration of social engineering methods, and the development of multi-circuit information protection systems.

2. Methods

The concept of a multi-contour security system for socio-cyber-physical systems, developed in previous studies [12], requires a suiTable threat classifier and a system security assessment model for practical implementation.

To build a classifier of socio-cyber-physical system threats, let's use the approach proposed in [12]. Let's introduce the following notations:

– define information resources as a set of plurals:

$$I_{A_i} = \left\{ Type_i, A_i^C, A_i^I, A_i^A, A_i^{Au}, A_i^{Inv}, \beta_i \right\},$$

where $Type_i$ – type of information asset, $Type_i$={CI_i, PD_i, CD_i, TS_i, StR_i, $PubI_i$, $ContI_i$, PI_i}, where CI_i – confidential information, PD_i – payment documents, CD_i – credit documents, TS_i – commercial secret, StR_i – statistical reports, $PubI_i$ – publicly available information, $ContI_i$ – control information, PI_i – personal data.

– security services will be defined as a plural:

$$A_i = \left\{ A_i^C, A_i^I, A_i^A, A_i^{Au}, A_i^{Inv} \right\},$$

where A_i^C – confidentiality, A_i^I – integrity, A_i^A– availability, A_i^{Au} – authenticity, A_i^{Inv} – involvement); β_i – metric of the ratio

of time and degree of information secrecy for the asset (critical – 1.0; high – 0.75; medium – 0.5; low – 0.25; very low – 0.01).

A web application was developed to determine the objectivity of expert evaluation and automation (https://skl.sspu.sumy.ua/login), which allows to form an expert assessment of the impact of the threat on the security service.

Table 1 shows the weighting coefficients of experts' competence (k_k). This approach allows to determine the consistency of the experts` opinions with varying degrees of knowledge in the field of cyber security and information protection. In addition, the proposed web application takes into account all components of the threat classifier shown in **Fig. 1**.

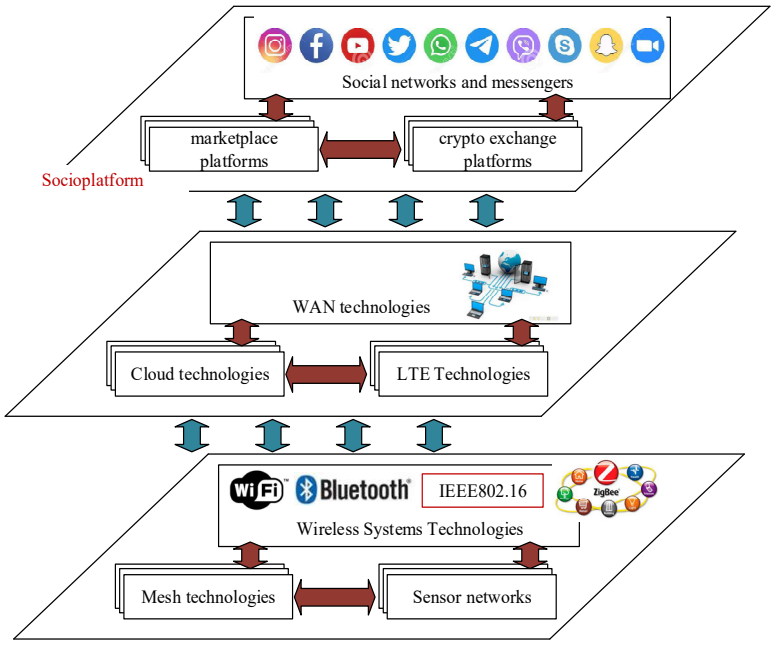

Fig. 1. Structural-logical scheme of socio-cyber-physical systems

The total assessment of the i-th threat is determined by the number of experts according to the expression:

$$\tilde{x}_i = \frac{\sum_{k=1}^{K} x_k \times k_k}{K}, \quad (1)$$

where x_k – evaluation of the k-th expert of the impact of the i-th threat; k_k – expert's competence level; K – number of experts.

Table 1
Weighting factor of experts' competence

Expert qualification	The value of the weighting factor (k_k)
International expert in the field of IS, CS, SI	1.0
National expert in the field of IS, CS, SI	0.95
Certified international specialist in the field of IS, CS, SI	0.9
Doctor of science in the field of IS, CS, SI	0.9
Head of the Security Service	0.85
PhD in the field of IS, CS, SI	0.8
A security officer	0.7
System administrator	0.6
Security service engineer	0.5
Postgraduate student with a specialty in the field IS, CS, SI	0.4

The measure of consistency of experts' assessments is the variance, which is determined by the expression:

$$\sigma_x^2 = \frac{1}{K}\sum_{k=1}^{K} k_k \left(x_k - \tilde{x}_i\right)^2. \quad (2)$$

Statistical probability of the obtained results $1 - \alpha_i$, will be:

$$\left[\widetilde{x_i} - \Delta, \widetilde{x_i} + \Delta\right],$$

where the value x_i distributed according to the normal law with center y and variance σ_X^2. Then Δ is defined by the expression:

$$\Delta = t\sqrt{\sigma_x^2 / N}, \quad (3)$$

where t – value according to the Student's distribution for k–1 degrees of freedom.

To form a multi-contour information protection system, let's use the mathematical apparatus for building multi-circuit security systems developed in [12]. At the same time, let's take into account signs of synergism and hybridity of mixed and targeted attacks on each of the platforms of socio-cyber-physical systems (on internal and external contours) (**Fig. 3**).

3. Results

The classifier consists of a tuple that includes the following components (**Fig. 2**):

– the level of criticality of the threat is determined by the set:

$$L_{kr_i} = \left\{L_{kr_1}, L_{kr2}, L_{kr3}, L_{kr4}, L_{kr5}\right\},$$

where L_{kr_1} – 01 (critical), L_{kr2} – 02 (high), L_{kr3} – 03 (medium), L_{kr4} – low, L_{kr5} – very low;

– the security component is defined by the plural:

$$S_i^{syb} = \left\{S_1^{syb}, S_2^{syb}, S_3^{syb}\right\},$$

where S_1^{syb} – 01 (cybersecurity), S_2^{syb} – 02 (information security), S_3^{syb} – 03 (security of informational);

– the component of security services is defined by the plural:

$$S_i^{serv} = \left\{S_1^{serv}, S_2^{serv}, S_3^{serv} S_4^{serv}, S_5^{serv}\right\},$$

where S_1^{serv} – 01 (A_i^I – integrity), S_2^{serv} – 02 (A_i^C – confidentiality), S_3^{serv} – 03 (A_i^A – availability); S_4^{serv} – 04 (A_i^{Au} – authenticity), S_5^{serv} – 05 (A_i^{Inv} – involvement);

– component of the nature of directions for the formation of security systems is determined by the plural:

$$S_i^{\text{influence}} = \left\{S_1^{\text{influence}}, S_2^{\text{influence}}, S_3^{\text{influence}}\right\},$$

where $S_1^{\text{influence}}$ – 01 (engineering and technical), $S_2^{\text{influence}}$ – 02 (organizational), $S_3^{\text{influence}}$ – 03 (legal and regulatory);

– the constituent layer of the ISO/OSI infrastructure is defined by the plural:

$$S_i^{ISO} = \left\{S_1^{ISO}, S_2^{ISO}, S_3^{ISO}, S_4^{ISO}, S_5^{ISO}, S_6^{ISO}, S_7^{ISO}\right\},$$

where S_1^{ISO} – 01 (physical level), S_2^{ISO} – 02 (network level), S_3^{ISO} – 03 (level of operating systems); S_4^{ISO} – 04 (level of applications and services), S_5^{ISO} – 05 (level of applications and services); S_6^{ISO} – 06 (the Internet of Things level), S_7^{ISO} – (the level of the information protection system);

– component of the direction of influence based on social engineering methods is defined by the plural:

$$S_i^{\text{sthreats}} = \left\{ S_1^{\text{sthreats}}, S_2^{\text{sthreats}}, S_3^{\text{sthreats}} S_4^{\text{sthreats}}, S_5^{\text{sthreats}} \right\},$$

where S_1^{sthreats} – 01 (hacking the system (subsystem, infrastructure element), S_2^{sthreats} – 02 (system compromise (subsystem, infrastructure element), S_3^{sthreats} – 03 (data compromise); S_4^{sthreats} – 04 (finding critical points of the system), S_5^{sthreats} – 05 (information gathering);

– the component of the safety circuit is defined by the plural:

$$S_i^{\text{safety loop}} = \left\{ S_1^{\text{safety loop}}, S_2^{\text{safety loop}} \right\},$$

where $S_1^{\text{safety loop}}$ – 01 (internal security contour), $S_2^{\text{ssafety loop}}$ – 02 (external security contour).

Thus, the proposed classifier of socio-cyber-physical system threats is defined as a set:

$$Q_j^{\text{sthreats}} = \left\{ L_{kr_i}, S_i^{syb}, S_i^{serv}, S_i^{\text{influence}}, S_i^{ISO}, S_i^{\text{sthreats}}, S_i^{\text{safety loop}} \right\},$$

where j – relevant threat, $j \in \forall \overline{1 \ldots N}$.

In **Fig. 3** $Q_{synerg_{1\,\text{platform}}}^{SCS\ ISL}$ – synergy of threats to the corresponding security service; α_i – the weighting factor of the possibility of threat implementation based on social engineering methods, $i \in \{0.25; 0.5; 0.75; 1.0\}$, where 0.25 – probability of using a threat based on social engineering methods 1 time per year (low level); 0.5 – probability of using a threat based on social engineering methods 1 time per month (average level); 0.5 – probability of using a threat based on social engineering methods 1 time per week (high level), 1.0 – probability of using a threat based on social engineering methods 1 time per day (critical level).

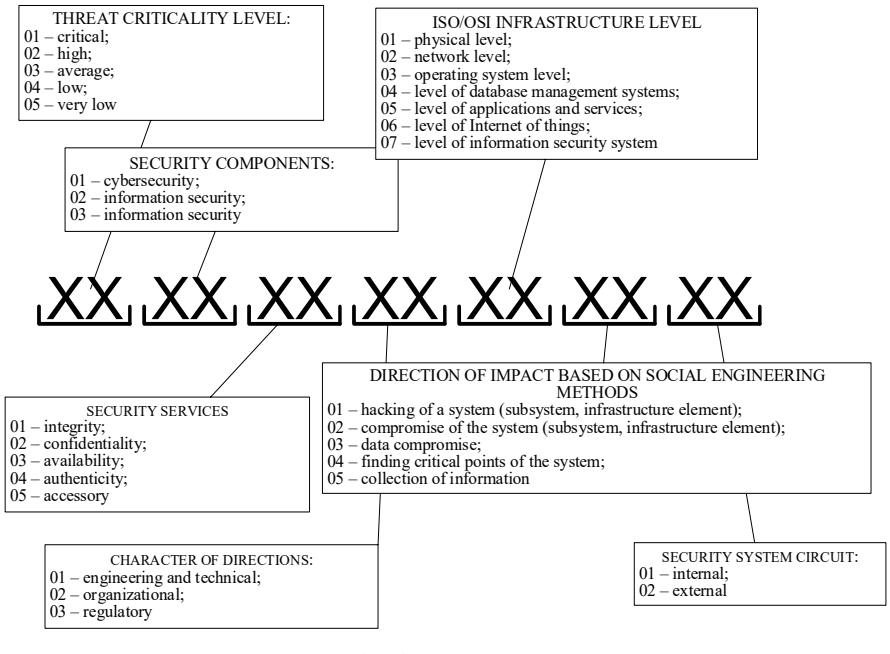

Fig. 2. Threat classifier for socio-cyber-physical systems

4. Discussion and scope of application

Based on the proposed approach to assessing the flow state of the security of system elements (infrastructure), the following method of assessing the security of socio-cyber-physical systems is proposed:

1 Stage. The formation of expert assessments of threats, their impact on security services, the possibility of signs of synergism and hybridity, as well as integration with social engineering methods. Determination of the impact of the threat on the infrastructure level (ISO/OSI models). At the same time, a matrix of weighting coefficients is formed

$$S_{\text{sthreats}}^{*} = \left\| S_{\text{sthreats}_{ij}} \right\|,$$

where i – security services, j – corresponding threat, $j \in \forall \overline{1 \ldots N}$.

2 Stage. Forming a correspondence matrix between information resources and security services:

$$S_{inf}^{*} = \left\| S_{inf_{il}} \right\|,$$

where i – security services, l – information resource, $l \in \forall \overline{1 \ldots L}$. When filling out the matrix, the need to provide the appropriate security service is taken into account (1 – the service is required, 0 – the service is not required).

3 Stage. Formation of dependence between information resources and infrastructure levels (ISO/OSI models) where information circulates and/or is stored:

$$S_{ISO}^{*} = \left\| S_{ISO_{kl}} \right\|,$$

where k – availability and type of communication, infrastructure element (level) where information is stored, l – information resource, $l \in \forall 1 \ldots L$.

4 Stage. Forming the dependence of threats and information resources (assessment of infrastructure criticality):

$$S_{\text{inf/sthreats}}^{*} = \left\| S_{inf_{lj}} \right\|,$$

where l – information resource, $l \in \forall 1 \ldots L$, j – corresponding threat, $j \in \forall 1 \ldots N$. This stage allows to determine the criticality of unauthorized access to one or another information resource.

5 Stage. Forming the dependence of threats and infrastructure elements (ISO/OSI model level):

$$S_{\text{sthreats/}ISO}^{*} = \left\| S_{\text{sthreats/}ISO_{kj}} \right\|,$$

where k – availability and type of communication, infrastructure element (level) where information is stored, j – corresponding threat, $j \in \forall 1 \ldots N$. The stage allows to identify critical points in the infrastructure and determine preventive security measures in advance.

6 Stage. Forming an assessment of the security of the socio-cyber-physical system based on the analysis of Stages 2 and 3 (finding the connection between information resources, infrastructure elements (critical points of unauthorized access/information leakage) and security services).

7 Stage. Forming an assessment of the capabilities of the current information protection system to resist threats:

$$S_{\text{sthreats/protection system}}^{*} = \left\| S_{\text{sthreats/protection system}_{qj}} \right\|,$$

where q – availability of a threat countermeasure mechanism, j – corresponding threat, $j \in \forall \overline{1 \ldots N}$.

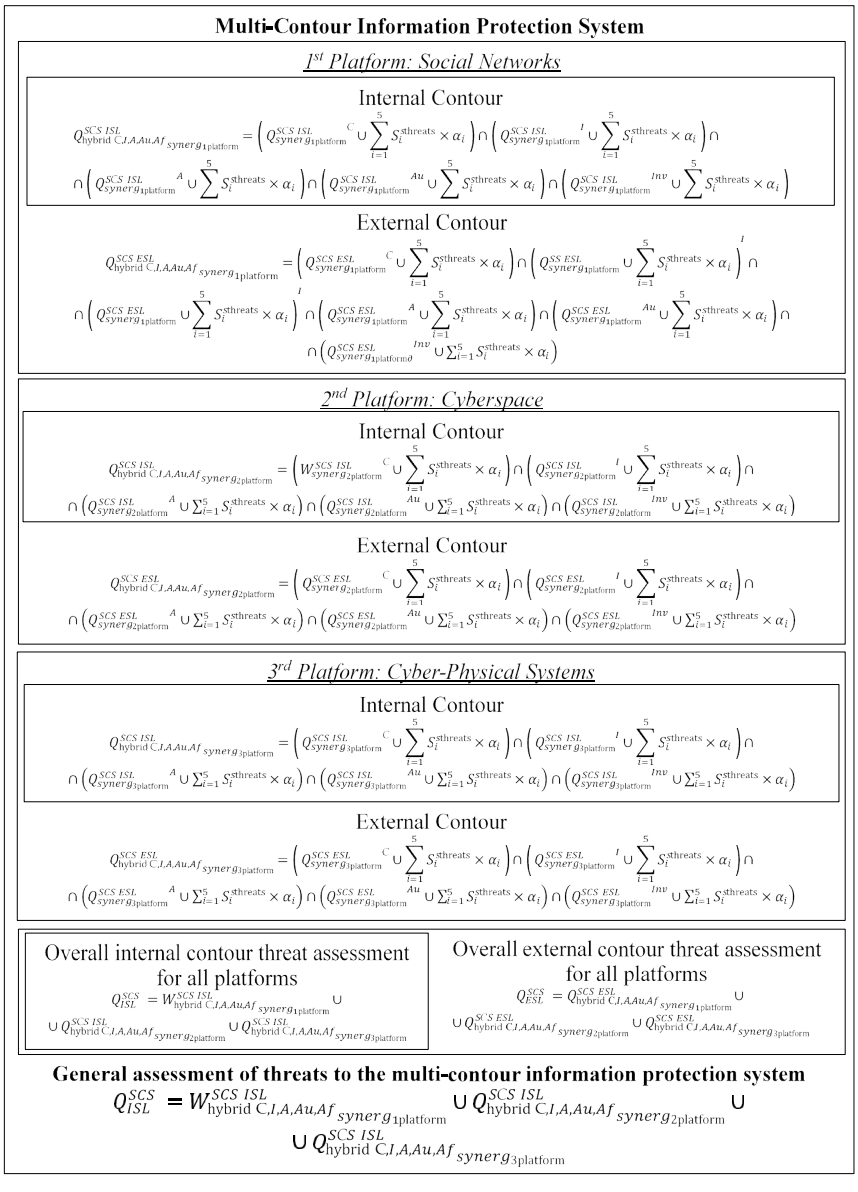

Fig. 3. Mathematical model of the multi-contour information protection system in socio-cyber-physical systems

8 Stage. Forming an assessment of regulators and legislation.

9 Stage. Forming an assessment of the flow state of the security system. At the same time, the results of Stages 6–8 are taken into account.

10 Stage. Calculation of the integral indicator of the current level of information security in the analyzed security system. For this, a comprehensive assessment of threats and the current state of the security system is calculated (Stage 9). After that, the absolute and relative value of the integral indicator is determined.

$$IS_{abs} = \frac{\sum S_{ij}}{i \times j}; \quad IS_{rel} = \frac{IS_{abs} - S_{\min}}{S_{\max} - S_{\min}}, \tag{4}$$

where IS_{abs} – the absolute integral indicator of the current state of information security in the security system; IS_{rel} – relative integral indicator of the current rooster of information security in the security system; S_{ij} – elements of the general system security assessment matrix; i – the number of rows of the general system security assessment matrix; j – the number of columns of the general system security assessment matrix; $S_{\min}$ – the minimum element of the overall system security assessment matrix; $S_{\max}$ – the maximum element of the overall system security assessment matrix.

In this way, it is possible to determine the overall integral assessment of the security of the system: the closer the value of the relative indicator is to 1, the higher is the overall security of information in the security system.

Hence, the suggested approach enables the consideration of the specified criteria for the classifier of threats within socio-cyber-physical systems, the operational status of the security system, and the prioritized adherence of management to the stipulations of both international regulatory bodies and domestic legislation.

5. Conclusions

The suggested threat classifier for socio-cyber-physical systems facilitates the consideration of characteristics related to the synergistic and hybrid nature of targeted (mixed) attacks, including their potential integration with social engineering methods. This approach enables the formulation of specific requirements and the development of multi-faceted information protection systems that factor in the platformability (structure) inherent in socio-cyber-physical systems.

The proposed methodology for evaluating the operational state of security systems in socio-cyber-physical systems provides a means to identify the financial implications associated with unauthorized access or loss of information resources. It also helps pinpoint critical infrastructure vulnerabilities and assess the effectiveness of information protection system mechanisms. Furthermore, the assessment of compliance with the mandates of international regulators and legislative acts serves to offer an unbiased evaluation of the security posture concerning continuous business processes.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

The study was performed without financial support.

Data availability

Manuscript has no associated data.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the current work.

References

1. IoT Security Maturity Model: Description and Intended Use. Available at: https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf
2. IoT Security Maturity Model (SMM): Practitioner's Guide. Available at: https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pdf
3. Lukova-Chuiko, N. V., Toliupa, S. V., Pogasiy, S. S., Laptieva, T. O., Laptiev, S. O. (2021). Improvement of the model of information protection in social networks. Collection of scientific works of the Military Institute Taras Shevchenko Kyiv National University, 73, 88–103. Available at: http://nbuv.gov.ua/UJRN/Znpviknu_2021_73_12
4. Pogasii, S. (2022). Models and methods of information protection in cyberphysical systems. Ukrainian Scientific Journal of Information Security, 28 (2), 67–79. doi: https://doi.org/10.18372/2225-5036.28.16951
5. Hryschuk, R. V., Danyk, Yu. G.; Dannik, Yu. G. (Ed.) (2016). Fundamentals of cyber security. Zhytomyr: ZhNAEU, 636.
6. Pogasii, S. (2022). Assessment of the level of security in cyberphysical systems. Ukrainian Information Security Research Journal, 24 (2), 81–94. doi: https://doi.org/10.18372/2410-7840.24.16933
7. Pohasii, S. (2021). Detection illegal of means of obtaining of information by the method of determining the deviation of the characteristics of radio signal from the specified parameters. Znanstvena misel journal, 1 (6), 23–29.
8. Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A., Mykus, S. et al. (2021). Development of a concept for building a critical infrastructure facilities security system. Eastern-European Journal of Enterprise Technologies, 3 (9 (111)), 63–83. doi: https://doi.org/10.15587/1729-4061.2021.233533
9. Yevseiev, S., Laptiev, O. L., Korol, O., Pohasii, S., Milevskyi, S., Khmelevsky, R. (2021). Analysis of information security threat assessment of the objects of information activity. International independent scientific journal, 34, 33–39. Available at: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/48505dd3-1a87-40fe-b9b1-e45f8f2bd72a/content
10. Pohasii, S. (2021). The mathematical model of information network protection based on hierarchic hypernetworks. Scientific discussion, 1 (61), 31–36.
11. Shmatko, O., Balakireva, S., Vlasov, A., Zagorodna, N., Korol, O., Milov, O. et al. (2020). Development of methodological foundations for designing a classifier of threats to cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 3 (9 (105)), 6–19. doi: https://doi.org/10.15587/1729-4061.2020.205702
12. Yevseiev, S., Murr, P., Milevskyi, S., Korol, O., Melnyk, M. (2023). Development of a Sociocyberphysical Systems Cyber Threats Classifier. 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). doi: https://doi.org/10.1109/ismsit58785.2023.10304895

Received date 08.09.2023
Accepted date 06.11.2023
Published date 29.11.2023

How to cite: *Milevskyi, S., Korchenko, O., Yevseiev, S. (2023). Socio-cyber-physical systems' threats classifier. Technology transfer: fundamental principles and innovative technical solutions, 16–20. doi: https://doi.org/10.21303/2585-6847.2023.003201*