Acta Montanistica Slovaca
ISSN 1335-1788
actamont.tuke.sk

Research on the assessment of the risk situations emergence for automated control systems of the metallurgical industry companies

Volodymyr SABAT[1], Bohdan DURNYAK[1], Lyubomyr SIKORA[2] and Volodymyr POLISHCHUK[3]**

Authors' affiliations and addresses:
[1] Ukrainian Academy of Printing, 19, Pid Holoskom St., Lviv, 79020, Ukraine
e-mail: v_sabat@ukr.net
e-mail: durnyak@uad.lviv.ua

[2] National University «Lviv Polytechnic», 12, Stepan Bandera St., Lviv, 79000, Ukraine
e-mail: email2@mail.com

[3] Faculty of Information Technology, Uzhhorod National University, Uzhhorod, Ukraine
e-mail: volodymyr.polishchuk@uzhnu.edu.ua

***Correspondence:**
Volodymyr Polishchuk, Uzhhorod National University, Narodna Square, 3, 88000, Uzhhorod, Ukraine
tel.: +380664207484
e-mail: volodymyr.polishchuk@uzhnu.edu.ua
Volodymyr Sabat, Ukrainian Academy of Printing, 19, Pid Holoskom St., Lviv, 79020, Ukraine
tel.: +380970366020
e-mail: v_sabat@ukr.net

How to cite this article:
Sabat, V., Durnyak, B., Sikora, L. and Polishchuk, V. (2023). Research on the assessment of the risk situations emergence for automated control systems of the metallurgical industry companies. *Acta Montanistica Slovaca*, Volume 28 (1), 201-213

DOI:
https://doi.org/10.46544/AMS.v28i1.16

Abstract
The article presents the assessment method of the risk situations emergence based on the analysis of the probability and frequency of threats emergence for automated control systems of the metallurgical industry companies (ACSMIC). The analysis of the risk dependency on vulnerabilities and threats to ACSMIC assets is carried out, and the relationship between risk, vulnerability, and threat is presented according to a three-level risk assessment scale. When identifying and assessing the risk, existing countermeasures against both external and internal attacks are taken into account, which, in turn, reduces the risk level for the protected organization. In the process of any organization functioning, there may be a need to reassess the risk associated with changes in the structure of the control organization or security policy in the system of the metallurgical industry companies. Therefore, the existing countermeasures are closely related to the concept of risk and require constant correction in the assessment process. Risk is related to the reliability of the functioning of the studied control structure of units and aggregates and their ability to function in accordance with the mode and goals of the production structure in various branches and levels of the hierarchy with an acceptable risk assessment. On the basis of the system concepts and assessment methods of the acceptable risk level, the system-oriented method of identifying the reliability of functioning of self-recovering complex hierarchical structures is proposed, the classification of the risk types of unforeseen situations in complex human-oriented systems that can be applied and implemented in hierarchical control systems is carried out.

Keywords
Metallurgical industry companies, threats, vulnerabilities, risks, management of hierarchical systems

Introduction

When studying risk, it is necessary first to define the concepts of assets, threats, and vulnerabilities for protected organizations or companies. If it is accepted that the company's assets are not of a permanent nature and can change their value in the functioning process, then there is a problem in the monetary equivalent of assessing the risk of losses in case of an incident of attacks or in case of their successful completion. On the other hand, the risk acquires a probabilistic nature due to a certain uncertainty of the emergence of a new threat related to the vulnerability of the company's assets, the goals that the agent sets for himself, having knowledge, access and motivation to carry out an attack on the hierarchical system, as well as the measures and countermeasures taken for assets protection from attacks. In order to conduct a risk assessment for a hierarchical control system, it is necessary to first study the relationship between vulnerabilities and threats for all possible access points to the information system and analyze the assets that contain these threats. According to the risk level assessment, it is possible to construct a protection system or modify it for new threats to improve the reliability and productivity of ACSMIC functioning with a hierarchical control structure (Victor Galaz et al., 2021).

At the current stage of development, the metallurgical industry company is a complex hierarchical infrastructure, which includes both assembly lines and automatic operational control systems, decision-making systems, expert groups, databases and knowledge bases, computer networks and automated workplaces (technological, administrative and managerial), which are connected into a single functional infrastructure. Accordingly, in case of threats and attacks, it is important to minimize the risks of production function failure.

In the era of the 4th industrial revolution, which the whole world has entered, Ukraine must also develop its own processing metallurgical industry, integrate the potential of high-tech sectors into it and find its place in the global world – not as a raw material, but as a high-tech and post-industrial state. Today, the main focus of the state policy is on integrating a number of projects into it that have already begun to develop in the regions in the areas of "Engineering – Automation – Mechanical Engineering" clusters and smart specialization. The challenge remains the same as in 2016 – much better consolidation of the various sectors and stakeholders of Industry 4.0 is needed to bring this strategy to the national level. At the same time, new trends bring new challenges. In his article (Klaus Schwab, 2016), Klaus Schwab writes that cyber security threats will increase. Therefore, the number of attacks and new threats to the automated control systems of the metallurgical industry companies will increase, as well as the number of risk situations for such systems.

In response to all these facts, it has been decided to conduct an actual scientific study, the main goal of which is to substantiate the assessment method of the risk situations emergence for the metallurgical industry companies based on the integration of information technologies and situational system analysis based on function coordination strategies.

The relevance of this study is confirmed by the introduction of data and knowledge assessment models in the EU to make balanced decisions in business, which is described in a European strategy for data for its implementation until 2030 (A European strategy for data, 2020).

Literature review

An analytical review of the problem of assessing the risks level and causes, which has a long history and is characterized by its methodology at various stages of research, as well as countermeasures to their emergence, is carried out. The problem of analyzing the causes of risk situations and emergency states of manufactured systems has its own specifics and appropriate research methods. For example, with regard to the methodology of the conducted research, one can point to the following methods, namely: in the work, the authors of (Stolyarov N., 2018) study the methods of describing information protection methods; the authors (Sabat V.I., 2014; Khoroshko V.O. et al., 2020) have performed the risk analysis in automated document management systems and synthesis of risk models; the authors of the work (Haley E.J. et al., 1984) have considered the issue of the risk level assessment in man-made systems based on the reliability concept; in a number of works (Syreyshchikova Nelli V. et al., 2019; Malyuk A.A., 2004; Ostapenko G.A., 2007) the methods and means of information technologies for constructing protection systems of various classes are substantiated; the works (Sabat V. et al., 2022; Durnyak B.V. et al., 2022) consider logical-cognitive and information technologies for increasing the security of control systems; the authors (Bobalo Yu.Ya. et al, 2020) consider the methods of constructing strategic level information protection systems and the risk level assessment. The book (Page S., 2017) proves that a group of experts will make better decisions about risk than individual specialists. The method of risk analysis and management (CRAMM Version 5.1 User Guide, 2021), which was presented by the central computer and telecommunications agency, allows risk analysis and control based on assessments assigned to resources, threats and vulnerabilities of resources. The following OCTAVE method (Alberts, C. et al., 2021) allows one to assess risk through the perspective of expected loss, without assessing probability, using a qualitative high/medium/low scale. There is also a risk assessment approach that uses ontology-based modelling (Palmer C. et al., 2018; Mozzaquatro, B.A. et al., 2018), and it uses semantic elements identified during risk analysis, which is a simple

and understandable way. A promising method for the risks assessment of automated control systems is the artificial neural network approach, which solves the problems of the above methods, in particular regarding flexibility and adaptability, but it requires a lot of intellectual resources for training networks (Paltrinieri, N. et al., 2019; Changwei, Y. et al., 2019). Nevertheless, these methods have not been fully tested for the metallurgical industry companies regarding the risk situations assessment for automated control systems.

With the rapid development of information and innovative technologies, there is an opportunity for early warning about risks and system security using computer technology. The risk of emergencies has always been the main factor limiting the sustainable development of companies in the metallurgical industry. Many studies focus on the study of risk assessment methods in various industries. For example, Polishchuk V. et al. (2021) developed a methodology for identifying the process controllability level in complex systems, taking into account risk-oriented factors of influence, which can be adapted for the metallurgical industry companies. The authors of (Paul Loft et al., 2022) consider increasing the accuracy of the assessment of information security risks of organizations through the implementation of corporate architecture. A safety assessment system is constructed based on dynamic Bayesian networks (Wang, Y. et al., 2010), which can be easily adapted to the metallurgical industry companies. The paper (Wu F. et al., 2021) presents highly reliable software systems used to prevent failures and increase the safety of automated control systems. The work (Xie, X.C. et al., 2019) presents an intelligent software platform for improving the quality of threat analysis of business processes by combining hazard and performance studies, the analysis of the protection level, and taking into account security requirements for completeness. Coal-mining and metallurgical companies have implemented information systems for labour protection management, which is also one of the elements of risk assessment (Yan X. et al., 2020; Zhang J.Q. et al., 2019).

Nevertheless, it can be stated that at the current stage, no comprehensive study of the risk situations assessment for automated control systems of the metallurgical industry companies has been presented.

Material and Methods

The process of risk assessment necessarily contains elements of predicting the future and, accordingly, the presence of many factors of uncertainty that are not foreseen in advance. Uncertainty is a rather broad concept that reflects the objective impossibility of obtaining absolute knowledge about the system's functioning's internal and external conditions and its parameters' ambiguity. Risk assessment uses methods of probability theory to represent uncertainty. In this context, the events that can occur are divided into permanent, periodic and random. The first two types of events are determined (deterministic), but the probability of random variables is also a precise mathematical concept and is defined explicitly. The probability theory can be used to represent uncertainties, despite the fact that these uncertainties can have different forms.

Although the term "probability" has a precise mathematical definition, its meaning, when used to represent uncertainties, is subject to various interpretations. Thus, *a frequentist probability* is considered to be the system's tendency to a certain manifestation in a theoretically infinite number of trials, i.e.:

$$P(A) = \lim_{n\to\infty}\left(\frac{X}{n}\right), \tag{1}$$

where $P(A)$ — is a probability of an event; A; X — a frequency of an event; n — the number of absolutely identical trials.

However, the frequency interpretation of probability cannot always be used in risk assessment. This refers to events that have not been observed in the past; therefore, it makes sense to assert the realization of these events only in the future. This especially applies to projects that involve the use of fundamentally new equipment and technologies. As fundamental research has shown, the probability theory can be interpreted differently from the statistical one. This interpretation was called *subjective* or *Bayesian probability*. Subjective probability is associated with a certain type of human decision-making behaviour and is not used to calculate other frequencies but to predict decision-making behaviours. By interpreting the theory for one decision-making situation, it is possible to predict the decision-makers actions in other situations. If it acts according to the probability theory, then the prediction turns out to be correct. Therefore, the *subjective probability* is considered the conviction degree in the feasibility of event A, the value of which is taken a priori. This view of probability is often used in various areas of science and technology and enables the use of professional expert assessment in the form of a numerical value of subjective probability and insufficient statistical data on the frequency of this or that event. Mathematically, subjective probability can be operated on like any other probability.

Under company assets, one will understand the company's information or resources and the control system's structure, which are subject to protection.

Definition 1. Risk is a fundamental concept in the protection system, which allows for identifying weak points and taking countermeasures for their localization and neutralization.

Definition 2. Risk is the loss probability that requires protection; in the absence of influences from external and internal threats, protection is not required.

Definition 3. Threats are any circumstances or events that may cause a violation of the information security policy and/or damage to assets, the structure of the control system, and the aggregated technological process.

Definition 4. System vulnerability is the system's inability to counteract a certain threat or set of threats. (Stolyarov N., 2018).

Together, these components form the basis of risk (Sabat V.I., 2014). Let one present the relationship of the main concepts in Fig.1, where S_{nz} —is the threat scale; S_V —— is the vulnerability scale; S_r — is the risk scale.

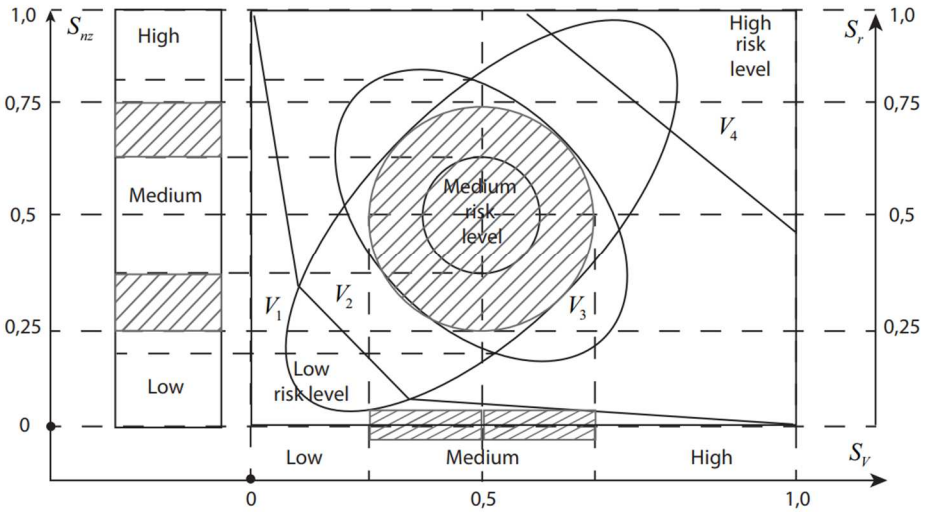

Fig. 1. Relationship between risk, vulnerability and threat

As seen in Fig.1, a three-level risk scale can be introduced for the relationship between threats and vulnerabilities, which is usually sufficient for its assessment.

Definition 5. Low risk refers to the security system condition in which an attacker needs to spend significant effort and expense to attack an organization but can only achieve minor results that do not cause significant damage to the organization.

In this case, the risk can be qualified within acceptable limits, and the security services make corrections in the protection system only when the risk level exceeds the acceptable norms defined by the security policy.

Definition 6. A medium risk level indicates that the threat is beyond the acceptable limits and can lead to attacks due to the organization's vulnerabilities, so measures must be taken to reduce the risk level to acceptable norms (low level).

If proper countermeasures are not taken in a timely manner, the risk level may increase to a high level. In case of high-risk levels, it is necessary to take constructive and safety measures to reduce them. Otherwise, it can lead to the direct performance of attacks in the weakest link of the organization's defence system. Attacking agents will take advantage of this by scanning the system for its high vulnerability due to an existing threat and performing an attack that will cause significant damage to the organization.

When identifying and assessing the risk, it is also necessary to take into account the existing countermeasures against both external and internal attacks. They, in turn, reduce the risk level for the organization. However, in the process of functioning in any organization, or production system, there may be a need to reassess the risk associated with changes in the structure of the management organization or security policy. Therefore, existing countermeasures are closely related to the concept of risk and require constant correction in the assessment process.

The concept of risk is related to the concept of the reliability of the functioning of the studied control structure of units and aggregates and their ability to function in accordance with the mode and goals of the production structure in various branches and levels of the hierarchy with an acceptable risk assessment.

In accordance with the analysis goals, various methods and concepts of identifying the acceptable level of emergency risk and reliability of information system functioning have been developed (Table 1).

Risk assessment managers make decisions based on risk assessment and other components, including economic, political, environmental, legal, reliability, productivity, safety and other factors. The answer to the question: "What security is sufficient?" is ambiguous and constantly changing in accordance with changes in the perception and understanding of risk. In order to identify "acceptable risk", managers need to analyze various options for the best choice. In some industries, the acceptable risk is identified through negotiation. For example, the US Nuclear Regulatory Commission requires that the reactor design be such to ensure reliability, stability and functional control, robustness to disturbances during the entire operational cycle and be checked at all stages of energy generation in accordance with the nuclear safety standards of reactors (Haley E.J. et al., 1984).

Table 1. *System concepts and methods for identifying the acceptable risk level*

Method	Short description	Class
Risk conversion factors	This method reflects the community's attitude to risk by comparing risk categories. It also provides an assessment for accepting risk conversion values between different risk categories	Cognitive
Farmer's curve	It represents the dependency of the risk profile (cumulative probability) for certain consequences (for example, deaths). It graphically shows the area of risk acceptance/rejection.	Cause and effect
Defining benefits	By comparing the risk and benefits of the activity, this method categorizes social preferences for voluntary and forced subjection to risk.	Goals balance
Assessment of consequences significance	It compares the risk probability and the significance of the consequences for different industry categories to identify the acceptable risk level.	Reliability
Effectiveness of risk reduction	It establishes the relationship between costs and the degree of risk reduction. If the costs exceed the benefits of risk reduction, then risk reduction measures are not applied. This may not coincide with societal notions of safety.	Economic
Risk comparison	The method compares different types of activity, industries, etc. and is best suited for comparing risks of the same type.	Process

Another way to assess risk acceptance is to identify the effectiveness of risk reduction based on the selection of an effective strategy:

$$\exists Strat\left(\frac{U}{C_i}\right):\left\langle E_{zR}=\left|\frac{V_{zR}}{\triangle R}\right|,\triangle R\to max\triangle r,\triangle r\subset I_{rd}\right\rangle, \tag{2}$$

where V_{zR} — are risk reduction costs; $\triangle R$ — is a reduction in the risk level, where: $\triangle R = R_{dz} - R_{pz}$, where R_{dz} — is the risk before measures to reduce it; R_{pz} — is the risk after measures to reduce it; $max\triangle r$ — is the degree of risk reduction; I_{rd} — is the permissible interval of action of the risk reduction measures. $\triangle R$ is also called the benefit obtained as a result of the risk reduction process. The risk reduction effectiveness E_{zR} can be used to compare several risk reduction attempts (Fig. 2).

In accordance with the system concept of the risk level assessment, the risk types and their characteristics can be classified according to the goals of the hierarchical structure functioning (Table 2).

Table 2. *Classification and characterization of the risk types of unforeseen situations in complex human-oriented systems*

Risk types	Risk object	Risk source	Risk event	α_{risk}
Individual	Man	Conditions of human activity	Illness, injury, disability, death	Cognitive $\alpha_{rk} \in [0{,}0 \div 1{,}0]$
Manufactured	Technical system	Technical imperfection, violation of operating rules	Accident, catastrophe	Project $\alpha_{rt} \in [0{,}0 \div 1{,}0]$
Ecological	Ecological systems	Anthropogenic intervention in the environment, technogenic emergency situations	Anthropogenic ecological disasters, natural disasters	Threats $\alpha_{rz} \in [0{,}0 \div 1{,}0]$
Social	Social groups	Emergency situation, deterioration of the life quality	Group injuries, diseases, increased mortality	Mental $\alpha_{rm} \in [0{,}5 \div 1{,}0]$
Economical	Material resources	Increased danger of production or the environment	Increase in security costs, damages from insufficient security	Resource $\alpha_{rr} \in [0{,}5 \div 1{,}0]$

A number of risk assessment methods have been developed based on the centuries-old practice of analyzing the risk's causes and methods of assessing their level (emergency, marginal, permissible, minimally permissible, cognitive in the processes of control and system design).

But the problem of resilience, that is, the restoration of system functions after active attacks on resources, structure and control processes, at high levels of risk: $\{\alpha_r(t_i, T_m, A_i) \to 1{,}0\}$, aбo $\{\alpha_r(t_i, T_m, IA_i)"\alpha_d\}$ is not fully resolved because the strategic goals of the threats are unknown in such cases.

Individual risk is determined by the probability of a potential danger implementation in case of a risk event emergence. Individual risk can be *voluntary* if a person's activity determines it voluntarily and *forced* if a person is exposed to risk as a part of society (for example, living in a polluted area and near objects of increased danger). Sources of individual risk and risk events that initiate it determine the cognitive influence on decision-making at all levels of the production hierarchy and society and administrative management.

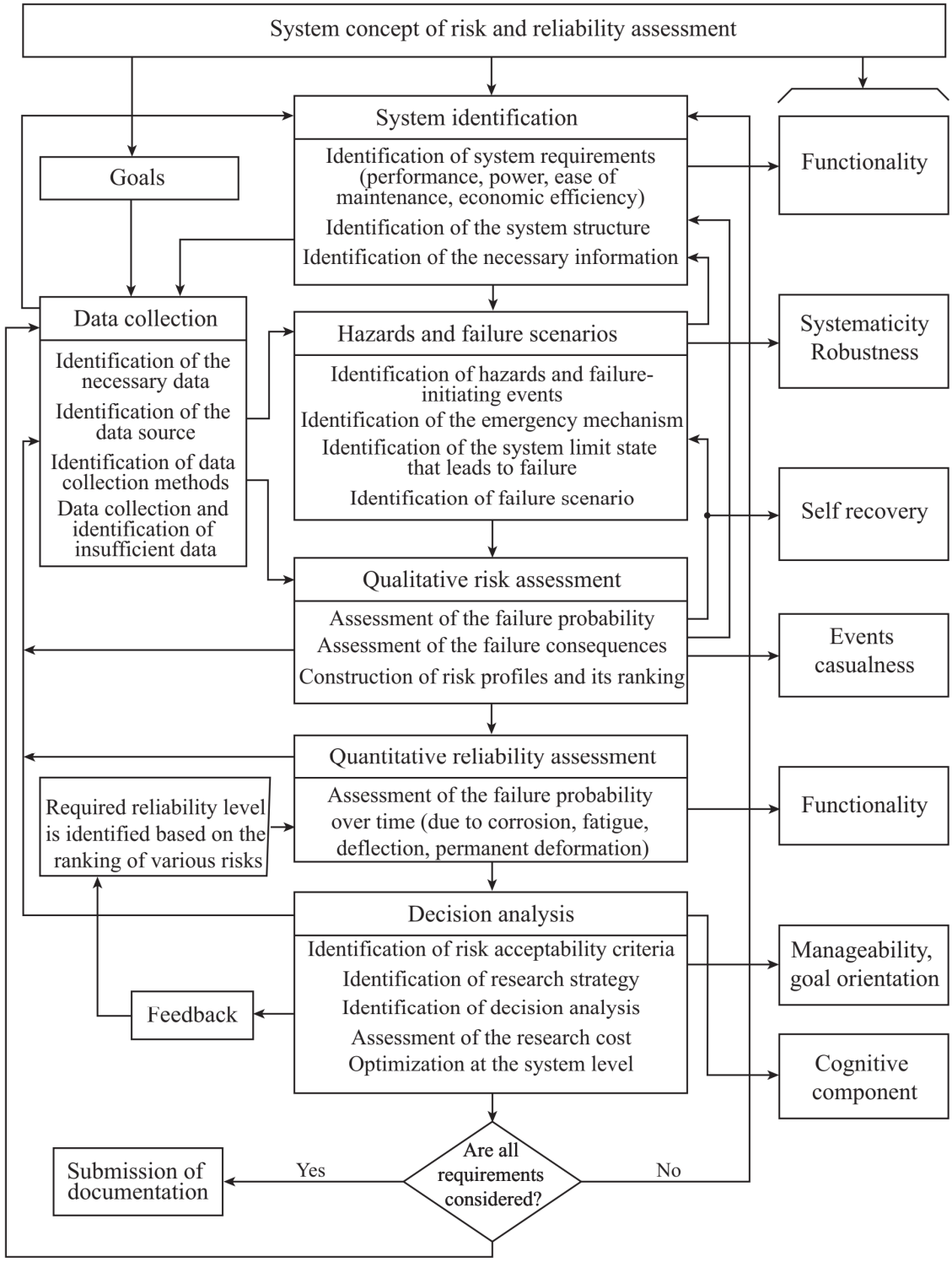

Fig 2. A system-oriented method of identification of the reliability of functioning of self-recovering complex hierarchical structures and assessing the risk level

Result

The results of the study have been tested on real data regarding the assessment of the probability of threats emergence to the automated control systems of the metallurgical industry companies. In the process of research into the probability of threats emergence to ACSMIC, a survey of system administrators of the metallurgical industry companies of Ukraine has been conducted in order to increase the reliability of assessing the probability of implementation and the threats emergence frequency to the company assets. Real survey data was collected from January to October 2021 through the cooperation of various organizations. Respondents were sent a diagram of dependencies between ACSMIC assets, a table with a list of ACSMIC assets and threats, and were asked to

assess the criticality, probability and frequency of threats emergence for each ACSMIC asset, taking into account dependencies between assets. The probability was assessed according to the following scale: 0 — the threat cannot be realized for this asset; 1 — low probability of threat emergence; 2 — the average probability of threat emergence; 3 — a high probability of threat. As a result of the surveys, the most common threats were identified, which have the highest probability of emergence for such assets:

- local networks;
- servers;
- mobile personal computers;
- workstations;
- ACSMIC software modules;
- supporting software;
- central database;
- internal data for the control of the metallurgical industry company;
- hard copies (hard drives, CDs, flashcards);
- document archives;
- output files;
- services provided by ACSMIC;
- the prestige of the organization.

The analysis of the results was carried out according to the principle of "maximum assessment"; that is, the highest assessment was selected from a number of assessments of one indicator of threats or vulnerabilities of the asset. The list of threats included threats related to various risk categories and functions (cognitive, systemic, informational). Table 3 shows the attacking agent's most common threats and actions, which have the maximum probability of detection for the company's assets.

Table 3. *Probability of threats emergence to ACSMIC assets*

Threat	Probability of threat emergence to ACSMIC assets												
	Networks	servers	Mobile PC	Workstations	Software modules	Supporting software	Central database	Internal data	Hard copies	Archives	Output files	Services	Prestige of organization
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Human physical threats aimed at the information system resource (IS)													
Disclosure, transfer or loss of access delimitation attributes	0	3	3	3	3	3	3	3	3	0	3	3	3
Human physical threats aimed at IS communication channel													
Cable damage	3	0	0	0	1	1	1	1	0	0	3	3	3
Global physical threats aimed at IS													
Natural disasters, artificial disasters, military operations, terrorist act	1	1	1	1	1	1	1	1	1	1	1	1	1
Local physical threats aimed at IS													
Failure of external and internal (reserve) sources of power supply, sharp voltage fluctuations in the power grid	3	3	3	3	0	0	0	0	0	0	0	3	3
Physical threats connected with the equipment failure													
Loss of information as a result of the failure of data carriers, defective data carriers	0	3	3	3	3	3	3	3	2	2	2	3	3
Local logical threats aimed at the operating system (OS)													
Launching the OS from external media, modifying OS components, refusing OS maintenance	0	0	0	0	2	3	3	3	2	0	2	3	3
Local logical threats aimed at software													
Opening files with macro viruses, modifying application software	0	0	0	0	2	3	3	3	2	0	2	3	3
Local logical threats aimed at information, which is stored and processed on the resource													
Unauthorized modification of information in the database stored on the resource	0	0	0	0	0	0	3	3	3	0	3	3	3
Remote logical threats aimed at OS													
Running exploits using remote OS vulnerabilities	0	0	0	0	1	1	1	1	0	0	1	1	1
Remote logical threats aimed at network services													
Running exploits that use remote vulnerabilities in network services and lead to the execution of arbitrary code on a remote PC	0	0	0	0	0	1	1	1	0	0	0	1	1
Logical threats aimed at network equipment													

Unauthorized access to a network device at the software level	1	0	0	0	1	1	1	1	0	0	1	1	1

1	2	3	4	5	6	7	8	9	10	11	12	13	14
Threats connected with physical and psychological effects on a person													
Decreased response to incidents due to administrator incapacity	1	1	1	1	1	1	1	1	1	0	1	1	1
Threats related to spy activity													
Disclosure, modification and substitution of confidential information by company employees	0	0	0	0	0	1	1	1	0	0	1	1	1
Threats related to unintended actions of personnel													
Accidental deletion of critical information	0	0	0	0	3	3	3	3	3	3	3	3	3

The frequency of threats emergence

For further risk assessment, the frequency of threats emergence during a certain period should be assessed. Table 4 shows the frequency of threats emerging to ACSMIC assets during the year. The frequency of emergence is assessed according to the following scale: 0 — the threat does not occur for this asset; 1 — the low frequency of threat emergence; 2 — the average frequency of the threat emergence; 3 — the high frequency of threat emergence.

Table 4. *Frequency of threats emergence to ACSMIC assets during a year*

Threat	*Frequency of threats emergence to ACSMIC assets during a year*												
	Networks	servers	Mobile PC	Workstations	Software modules	Supporting software	Central database	Internal data	Hard copies	Archives	Output files	Services	Prestige of organizatio
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Human physical threats aimed at the information system resource (IS)													
Disclosure, transfer or loss of access delimitation attributes	0	3	3	3	3	3	3	3	3	0	3	3	3
Human physical threats aimed at IS communication channel													
Cable damage	1	0	0	0	1	1	1	1	0	0	1	1	1
Global physical threats aimed at IS													
Natural disasters, artificial disasters, military operations, terrorist act	0	0	0	0	0	0	0	0	0	0	0	0	0
Local physical threats aimed at IS													
Failure of external and internal (reserve) sources of power supply, sharp voltage fluctuations in the power grid	3	3	3	3	0	0	0	0	0	0	0	3	3
Physical threats connected with the equipment failure													
Loss of information as a result of the failure of data carriers, defective data carriers	0	2	2	2	2	2	1	2	0	0	2	2	2
Local logical threats aimed at the operating system (OS)													
Launching the OS from external media, modifying OS components, refusing OS maintenance	0	0	0	0	3	3	3	3	3	0	3	3	3
Local logical threats aimed at software													
Opening files with macro viruses, modifying application software	0	0	0	0	3	3	3	3	3	0	3	3	3
Local logical threats aimed at information, which is stored and processed on the resource													
Unauthorized modification of information in the database stored on the resource	0	0	0	0	0	0	3	3	3	0	3	3	3
Remote logical threats aimed at OS													
Running exploits using remote OS vulnerabilities	0	0	0	0	2	2	2	2	0	0	2	2	2
Remote logical threats aimed at network services													
Running exploits that use remote vulnerabilities in network services and lead to the execution of arbitrary code on a remote PC	0	0	0	0	0	2	2	2	0	0	0	2	2
Logical threats aimed at network equipment													
Unauthorized access to a network device at the software level	1	0	0	0	1	1	1	1	0	0	1	1	1
Threats connected with physical and psychological effects on a person													
Decreased response to incidents due to administrator incapacity	1	1	1	1	1	1	1	1	1	0	1	1	1
Threats related to spy activity													
Disclosure, modification and substitution of confidential information by company employees	0	0	0	0	0	1	1	1	0	0	1	1	1
Threats related to unintended actions of personnel													
Accidental deletion of critical information	0	0	0	0	3	3	3	3	3	3	3	3	3

Thus, based on the analysis of the data in Tables 3, and 4, a list of threats to ACSMIC is received, which may occur with a medium or high probability and cause significant damage to one or several assets, which will lead to significant violations in the work of ACSMIC.

When analyzing the threats emergence frequency in the work of ACSMIC (from the above during the year), it is possible to single out the following 10 threats that occur most often:

1. Failure of external and internal sources of energy supply;
2. Sharp voltage fluctuations in the grid;
3. Loss of information due to the failure of data carriers or their defects;
4. Running files with viruses that operate on OS, including from external media;
5. Modification of OS components;
6. Failure of OS maintenance;
7. Opening files with macro viruses;
8. Application software modification;
9. Failure in software maintenance;
10. Threats related to unintended actions of personnel.

Vulnerability assessment

When assessing vulnerabilities, the concept of vulnerability is taken into account as a property or attribute of an asset that can be used in a different way or for other purposes than those for which this asset is intended. This type of assessment involves the identification of vulnerabilities in the environment, organization, procedures, personnel, management, administration, hardware, software, or communication equipment that a threat source could use to cause damage to the organization's assets and business activities. By itself, the presence of vulnerabilities does not cause damage since this requires the presence of a corresponding threat and an attack that uses it. The presence of a vulnerability in the absence of such a threat does not require the use of protective measures, but the vulnerability should be recorded and further tested in case the situation changes. It should be noted that improperly used, or malfunctioning security measures can become sources of vulnerabilities. (Sabat V. et al., 2022).

To assess vulnerabilities, a specialized IS vulnerability catalogue of "Digital Security" is used. The assessment of vulnerabilities will be carried out only for the threats given in the work since it does not make sense to assess vulnerabilities for non-critical threats, as well as for those that emerge with a very low probability. Table 5 presents a list of vulnerabilities for all critical threats and an assessment of the probability of vulnerability implementation. The probability is assessed according to the following scale: 1 — low probability of vulnerability implementation; 2 — average probability of vulnerability implementation; 3 — high probability of vulnerability implementation.

Table 5. *Vulnerabilities assessment*

Threat	Vulnerabilities of ACSMIC used by the threat	Probability of vulnerability implementation to the
1	2	3
Human physical threats aimed at IS resource		
Unauthorized use of equipment	Absence of pass systems for staff and one-time visitors	2
	The object's security system does not meet modern requirements, or there are ways of unauthorized access to the protected area	1
	Lack of regulations for access to premises with resources that contain valuable information	1
	Lack of control over personnel handling resources with valuable information	1
	Absence of the object surveillance system	1
	There is no periodic inspection of premises with resources containing valuable information for the presence of technical means of intelligence	1
	Lack of instructions for the staff regarding the use of the company's equipment	3
	Lack of access control system to the equipment	3
Disclosure, transfer or loss of access delimitation attributes	Lack of procedures for regularly reviewing the list of persons who have access to premises with resources containing valuable information	1
	Absence of regulation for terminating an employee's access to a protected area in the event of dismissal	2
	Absence of instructions for staff regarding compliance with the company's pass regime	2
	Personal visual staff identifiers do not contain identifiable information that is highly distinguishable	1
	There is no periodic check of whether the access delimitation attribute belongs to an authorized employee	3

1	2	3
Human physical threats aimed at IS communication channel		
Cable damage	Power and telecommunication cables are not separated	3
	Critical telecommunication cables are not duplicated	3
	There are no means to detect an unauthorized connection to cable systems	1
	Critically important telecommunication cables are not protected by boxes	3
	There is no warning or explanatory marking on the cables for users	3
	Lack of cable shielding	2
	Critically important telecommunications cables are located in public areas	1
	Lack of instructions and markings for service personnel on cables and electronic equipment	3
Local physical threats aimed at IS		
Fire	Lack of reserve systems	3
	Lack of fire protection	1
	Fireproof safes are not used	1
	Flammable materials are located near resources with valuable information	3
Cross-reference	Lack of shielding	2
	Incorrect separation of power cables	3
Failure of external sources of energy supply	Lack of reserve systems	3
	Absence of duplicate energy supply sources	3
	Uninterruptible power supplies are not used	3
Failure of backup sources of energy supply	Lack of reserve systems	3
	Absence of duplicate energy supply sources	3
	Uninterruptible power supplies are not used	3
	Regular maintenance of uninterruptible power sources is not carried out	3
Sharp voltage fluctuations	Lack of reserve systems	3
	No network filters are used	3
	The permissible number of electricity consumers has been exceeded	3
Physical threats connected with the equipment failure		
Loss of information as a result of a failure of data carriers	Lack of reserve systems	3
	Lack of instructions for staff regarding the use of company resources	3
	There is no technical maintenance of data carriers	3
Defective data carriers	Data carriers are not checked after their purchase	3
	Absence of regulations for the purchase of new equipment	3
Decrease in equipment reliability	The equipment is not replaced in a timely manner	3
	Regular maintenance of the equipment is not carried out	3
	Non-observance of equipment operating conditions	3
Local logical threats aimed at OS		
Running files with viruses that operate on OS	Anti-virus software is not installed	2
	Anti-virus software is not regularly updated	2
	Typical errors when configuring the OS	2
	Lack of instructions for personnel regarding anti-virus protection of information resources	3
Launching the OS from external media	Availability of devices for reading external media	2
	Lack of instructions for staff on working with IS	3
	BIOS settings allow one to run the OS from external media	3
	It is possible to change BIOS settings; there is no password protection	3
Modification of OS components	Anti-virus software is not installed	2
	Anti-virus software is not regularly updated	2
	Lack of instructions for staff working with IS	3
	Lack of integrity control of executable files and OS system libraries	1
	The principle of least privilege is not followed when assigning user rights	2
OS service failure	Lack of backup of data processed by OS and OS settings itself in order to be able to deploy the operation of OS in a backup location	3
	Lack of OS recovery systems	3
	No OS recovery procedures	3
	Unstable operating systems are used on critical objects	1
	No network load balancing system is used	1
Local logical threats aimed at software		
Opening files with macro viruses	Anti-virus software is not installed	2
	Anti-virus software is not regularly updated	2
	Lack of instructions for personnel regarding anti-virus protection of information resources	3
	Typical errors in the configuration of interpreters	1
Modifying application software	Anti-virus software is not installed	2
	Anti-virus software is not regularly updated	2
	The principle of least privilege is not followed when assigning user rights	3
	Lack of integrity control of executable files and libraries of application software	1
	Absence of an approved list of application software permitted for use	3

1	2	3
Failure to service the application software	No network load balancing system is used	1
	Absence of an approved list of application software permitted for use	3
	Lack of instructions for testing and deploying the application software in the business environment	3
	Absence of recovery systems for working configurations of application software	3
	Absence of application software recovery procedures	3
	Unreliable application software is used at critical facilities	1
	Failure to meet the requirements of the application software for the hardware configuration, taking into account the maximum possible load	1
Local logical threats aimed at information, which is stored and processed on the resource		
Unauthorized modification of information in the database stored on the resource	Lack of reserve systems	3
	Lack of instructions for staff working with IS	3
	Lack of DBMS settings that ensure transaction security	1
	No transaction log	1
	Lack of authorization to make changes to the DBMS	1
	Lack of data and DBMS integrity control	1
	The workstation (terminal) is not locked when idle	1
Unauthorized modification of electronic documents containing valuable information	Lack of reserve systems	3
	Lack of instructions for staff working with IS	3
	The workstation (terminal) is not locked when idle	1
	An electronic digital signature is not used when forwarding electronic correspondence	3
	The absence of a secure document management system in the company	1
	No cryptographic data protection system is used	3
	Lack of regulations for working with the cryptographic data protection system	3
Loss or violation of the integrity of information due to incorrect operation of the software	Lack of reserve systems	3
	Lack of integrity control systems	1
	There is no software testing before implementation	2
	There is no regular check of the correct operation of the software	1
	Low qualifications of system administrators	2
Deletion of valuable information in the database by the attacker	Lack of reserve systems	3
	No transaction log	1
	The workstation (terminal) is not locked when idle	1
	Lack of authorization to access DBMS	1
	Lack of instructions for staff on working with confidential information	3
Deletion of electronic documents with valuable information by the attacker	Lack of reserve systems	3
	The workstation (terminal) is not locked when idle	1
	The absence of a secure document management system in the company	1
	Lack of instructions for staff working with confidential information	3
	Lack of authorization when accessing the resource	1
Threats related to unintended actions of personnel		
Violation of confidentiality of information due to inadvertent actions	The absence of a secure document management system in the company	1
	Job descriptions do not include liability for inadvertent actions	3
	Absence of mandatory informing of personnel about regulatory documents that regulate work with confidential information	3
	There is no regular verification of users' rights to access information resources	1
	Absence of confidentiality markers (vultures) on documents containing confidential information	3
Unintentional violation of information integrity	Lack of reserve systems	3
	The absence of a secure document management system in the company	1
	Job descriptions do not include liability for inadvertent actions	3
	Absence of mandatory informing of personnel about regulatory documents that regulate work with confidential information	3
	There is no regular verification of users' rights to access information resources	1
	No mandatory authorization to modify confidential information	1
Accidental deletion of critical information	Lack of reserve systems	3
	The absence of a secure document management system in the company	1
	Job descriptions do not include liability for inadvertent actions	3
	Absence of mandatory informing of personnel about regulatory documents that regulate work with confidential information	3
	There is no regular verification of users' rights to access information resources	1
	No mandatory authorization to delete information	1

Discussion

The research has been conducted, based on the identification of assets of the metallurgical industry companies and the dependency scheme between assets, according to the studies developed in the scientific work for printing industries (Sikora Lyubomir et al., 2021), where the criticality, probability and frequency of threats emergence are assessed for each asset of ACSMIC. As a result of the study, the most critical threats that occur most often during the year are identified. This, in turn, makes it possible to increase the protection and reliability level of ACSMIC by implementing proactive management to reduce the vulnerability and threats level to assets whose risk level

exceeds the permissible limits defined in the security policy. The shortcomings of the conducted research include the fact that when collecting data (2021), the metallurgical industry companies worked in the usual safe mode, and other modes of their operation were not taken into account, for example, martial law, restrictions on the use of energy resources, shelling, etc. After the full-scale invasion of enemy troops into Ukraine, such operation modes exist for the metallurgical industry companies. Of course, today, many of the parameters of asset studies listed in the tables are becoming critical, so in wartime, it is necessary to introduce their correction, which was not taken into account in peacetime. This limitation inspires the authors for future research in this area.

In the course of the conducted research, the definition of the concepts of risk, threat, and vulnerability in the concept of protection systems for company assets is proposed. The relationship scheme between risk, threat and vulnerability is substantiated and developed according to a three-level scale of risk assessment. Although a more flexible scale can be used for other studies, three risk levels are sufficient for this study: low, medium and high.

The concepts and methods for identifying the acceptable risk level and the effectiveness of reducing the risk of the system function loss in case of interference with the management process are analyzed, based on which a system-oriented method of identifying the reliability of the functioning of self-recovery complex hierarchical structures and risk assessment is proposed. The classification and characteristics of the risk types of unforeseen situations in complex human-oriented systems with the identification of their ranges of values in the formation of the total amount of risk in the range from "0" to "1" are presented.

The analysis of the probability of risks emergence in the process of managing complex systems with a hierarchical structure under the conditions of threats and vulnerabilities of assets of automated control systems of a metallurgical industry company during formation and decision-making is carried out, based on the study of the probability of threats emergence, the frequency of their repetition in the annual terminal period of production for the most used assets and their vulnerability to critical threats. The ten most probable threats for each of the assets are identified, which require taking necessary countermeasures to reduce the risk level within acceptable norms.

The study results are verified and tested on the real data of the survey of system administrators of the metallurgical industry companies of Ukraine. The rationality of the obtained results proves the advantages of assessing the emergence of risk situations. The reliability of the obtained results is ensured by the correct use of the logical-systemic approach, probabilistic methods, and selecting an effective strategy when identifying the risk level for assets and ACSMIC as a whole.

Conclusions

The research is conducted on the actual innovative task of substantiating the method of assessing the risk situations emergence for metallurgical industry companies, based on the integration of information technologies and situational system analysis on the basis of function coordination strategies. The following results are obtained:

- for the first time, a comprehensive definition of the risk of emergency situations is substantiated, the factors affecting the system control process and the system concept and methods for determining the acceptable level of emergency risk under an active attack or threat factors are identified;
- for the first time, a system-oriented method of identifying the reliability of the functioning of complex hierarchical structures is improved to counter risks in case of threats. The classification of risk types and infrastructure failure is carried out due to the system blocking of the automatic document management system, which is a part of the structure of automatic control systems of the metallurgical industry companies.

The research results can be implemented in the design of the control and protection system not only for ACSMIC but also for any complex systems with a hierarchical structure under threats and crisis situations, as well as for companies of other industries.

Further research of the problem can be seen in developing the software for the practical use of the developed model, as well as the research of the parameters of the assets in wartime.

References

A European strategy for data. (2020). Available at: https://ec.europa.eu/info/sites/default/files/communication-european-strategy-data-19feb2020_en.pdf

Alberts C., Dorofee A. OCTAVE Threat Profiles. Software Engineering Institute, Carnegie Mellon University. Available online: http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/AlbertsDorofee_OCTAVEThreatProfiles.pdf (accessed on 11 January 2021).

Bobalo Yu.Ya., Dudykevich V.B., Mykytyn T.V. Strategic security of the object — information technology system. Lviv: Lviv Polytechnic University, 2020. 260 p.

Changwei, Y.; Zonghao, L.; Xueyan, G.; Wenying, Y.; Jing, J.; Liang, Z. Application of BP Neural Network Model in Risk Evaluation of Railway Construction. Complexity 2019, 2019, 2946158.

CRAMM Version 5.1 User Guide; Insight Consulting: 2005. Available online: https://pdfcoffee.com/cramm-version-51-user-guide-pdf-free.html (accessed on 29 June 2021).

Durnyak B.V., Tkachuk R.L., Mashkov O.A., Sikora L.S., Lysa N.K. Information and logical-cognitive technologies for training operative personnel for work in terminal emergency situations. Lviv: UAD, 2022 314 p.

Haley E.J., Kumamoto H. Reliability engineering and risk assessment - M. : Mashinostroenie, 1984. 528 p.

Khoroshko V.O., Pavlov I.M., Bobalo Yu.Ya., Dudykevich V.B., Opirskyi I.R., Parkhuts L.T.. Design of complex information protection systems. Textbook. Lviv: Lviv Polytechnic Publishing House, 2020. 320 p.

Klaus Schwab. The Fourth Industrial Revolution: what it means, how to respond (Jan 14, 2016): https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond

Malyuk A.A. Introduction to the protection of information in automated systems. M. : Telekom, 2004. 147 p.

Mozzaquatro, B.A.; Agostinho, C.; Goncalves, D.; Martins, J.; Jardim-Goncalves, R. An Ontology-Based Cybersecurity Framework for the Internet of Things. Sensors 2018, 18, 3053

Ostapenko G.A. Information operations and attacks in sociotechnical systems. M. : Telekom, 2007. 134 p.

Page, S. (2017). The diversity bonus. In The Diversity Bonus. Princeton University Press.

Palmer, C.; Urwin, E.N.; Niknejad, A.; Petrovic, D.; Popplewell, K.; Young, R.I. An ontology supported risk assessment approach for the intelligent configuration of supply networks. J. Intell. Manuf. 2018, 29, 1005–1030.

Paltrinieri, N.; Comfort, L.; Reniers, G. Learning about risk: Machine learning for risk assessment. Saf. Sci. 2019, 118, 475–486.

Paul Loft, Ying He, Iryna Yevseyeva, Isabel Wagner, CAESAR8: An agile enterprise architecture approach to managing information security risks, Computers & Security, Volume 122, 2022, 102877, https://doi.org/10.1016/j.cose.2022.102877.

Polishchuk V. Methodology for determining the level of process control in complex systems taking into account risk-oriented factors from safe time to pandemics/ V. Polishchuk, M. Kelemen, M. Kelemen jr. // Proceedings of The Fourth International Workshop on Computer Modeling and Intelligent Systems (CMIS-2021) (Zaporizhzhia, 27 April 2021). – CEUR Workshop Proceedings, Vol. 2864, 2021 – P. 419-433 doi: http://ceur-ws.org/Vol-2864/paper37.pdf (Scopus)

Sabat V., Sikora L., Durnyak B., Lysa N., Fedevych O. Information techno¬logies of active control of complex hierarchical systems under threats and information attacks. The 3rd International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS-2022) Khmelnytskyi, Ukraine, May 25 – 27, 2022. (Scopus)

Sabat V.I. Analysis of risks in automated document circulation systems. Modeling and information technologies. Collection of scientific works. K.: IPME named after H. E. Pukhov, National Academy of Sciences of Ukraine, 2014. Vol. 73. P. 198–204.

Sikora Lyubomir, Lysa Natalia, Tkachuk Rostislav, Sabat Volodymyr, Fedevych Olga. Information Technology of Risk Assessment for Automated Control Systems of Printing Production. CITRisk'2021: 2nd International Workshop on Computational & Information Technologies for Risk-Informed Systems, September 16–17, 2021, Kherson, Ukraine: https://ceur-ws.org/Vol-3101/Paper30.pdf

Stolyarov N. Concept, essence, goals and meaning of information protection. Introduction. Sec4all. Safety for everyone. [[Cited from the network: 02.09.2018.] http://www.sec4all.net/infoprot-vved.html.

Syreyshchikova Nelli V., Pimenov Danil Yu., Mikolajczyk Tadeusz, Moldovan Liviu, Information Safety Process Development According to ISO 27001 for an Industrial Enterprise, Procedia Manufacturing,Volume 32, 2019, Pages 278-285, https://doi.org/10.1016/j.promfg.2019.02.215.

Victor Galaz, Miguel A. Centeno, Peter W. Callahan, Amar Causevic, Thayer Patterson, Irina Brass, Seth Baum, Darryl Farber, Joern Fischer, David Garcia, Timon McPhearson, Daniel Jimenez, Brian King, Paul Larcey, Karen Levy, Artificial intelligence, systemic risks, and sustainability, Technology in Society, Volume 67, 2021, 101741

Wang, Y.; Huang, L.S.; Yang, W. A Novel Real-Time Coal Miner Localization and Tracking System Based on Self-Organized Sensor Networks. Eurasip J. Wirel. Commun. Netw. 2010, 2010, 142092.

Wu, F.; Cheng, L.; Yu, Y.L.; Sun, J.J. Research on the index system of chemical enterprise safety risk state based on analytic hierarchy. In Proceedings of the 2021 5th International Conference on Advances in Energy, Environment and Chemical Science (AEECS 2021), Shanghai, China, 26–28 February 2021; Volume 245, p. 03082.

Xie, X.C.; Fu, G.; Xue, Y.J.Y.; Zhao, Z.Q.; Chen, P.; Lu, B.J.; Jiang, S. Risk prediction and factors risk analysis based on IFOA-GRNN and apriori algorithms: Application of artificial intelligence in accident prevention. Process Saf. Environ. Prot. 2019, 122, 169–184.

Yan, X.; Deng, X.W.; Sun, S.H. Analysis and Simulation of the Early Warning Model for Human Resource Management Risk Based on the BP Neural Network. Complexity 2020, 2020, 8838468.

Zhang, J.Q.; Chen, X.B.; Sun, Q.B. An Assessment Model of Safety Production Management Based on Fuzzy Comprehensive Evaluation Method and Behavior-Based Safety. Math. Probl. Eng. 2019, 2019, 413703