UDC 004.451.36:681.5

ANALYSIS OF RISK TERMINAL FLOWS IN TECHNOGENIC SYSTEMS ARISING IN THE PROCESS OF THREAT IMPACT

Sabat V. I. – PhD, Associate Professor, Associate Professor of the Department of Information Multimedia Technologies of Ukrainian Academy of Printing, Lviv, Ukraine.

Sikora L. S. – Dr. Sc., Professor, Full Member of the Engineering Academy of Ukraine, Professor of the Department of Automated Control Systems of the Institute of Computer Sciences and Information Technologies, Lviv, Ukraine.

Durnyak B. V. – Dr. Sc., Professor, Honoured Worker of Science and Technology of Ukraine, Rector of Ukrainian Academy of Printing, Lviv, Ukraine.

Povkhan I. F. – Dr. Sc., Professor, Dean of the Faculty of Information Technologies, Uzhhorod National University, Uzhhorod, Ukraine.

Polishchuk V. V. – Dr. Sc., Associate Professor, Professor of the Department of Systems Software, Uzhhorod National University, Uzhgorod, Ukraine.

ABSTRACT

Context. The analysis of the risk terminal flows in technogenic systems is carried out, which arise in the process of the impact of informational and cognitive threats in the automated document management system as part of the hierarchical production system.

The object of the research is the process of functioning of complex systems with a hierarchical structure, in which automated document management systems with a high level of data flow protection for decision-making are used to provide the information quality control of technological processes.

The subjects of the research are the methods and means of constructing an information protection system to ensure the reliable functioning of automated document management systems and making targeted decisions in hierarchical structures with minimal risk of exposure to external threats and attacks.

Objective is to develop a complex model for assessing the risk of the document management system failure as part of a hierarchical production system under the active threats.

Method. For the first time, the cause-and-effect diagram of the event formation with the active action of threat factors and attacks is substantiated and developed, the interpretation of risk in a technogenic system is defined, and the risk in the space of states is presented as a change in the trajectory in the system transitions to the limit operation mode. For the first time, a category diagram of the structure of risk generation under the threat factors and a system-category diagram of interaction in the system *risk ↔ emergency-active nature* is constructed, a system-category scheme of risk formation under the active threat factors is suggested. For the first time, a cognitive diagram for assessing losses in the event of a risk situation arising from incorrect actions of the personnel is substantiated.

Results. As a result of the research, a system-category diagram of the impact of a set of threats on the system functioning mode and process is constructed, a method is developed for calculating the level of system strategic security of energy-active hierarchical systems in the process of attacks and threats, and a complex model for assessing the risk of a system functioning failure under active threats is suggested.

Conclusions. Under the action of active obstacles, cognitive and system factors at the operational and strategic levels of the control hierarchy, due to wrong decisions and informational disorientation, emergency situations and risks of the system function loss and its target-orientation arise. The analysis of a set of risks and the suggested category diagram of the risk generation structure under the impact of threat factors form the basis of the development of the probability structure of the risk concept based on the *attack ↔ consequence* model, as well as the construction of a system-category diagram of the interaction in the game *active factor ↔ accident risk*. This, in turn, makes it possible to construct a system-category scheme for the formation of risk terminal flows in technogenic systems that arise in the process of threat impact. A complex model for assessing the risk of system failure under threats can be used to construct protection systems for any hierarchical control structures of technogenic systems.

KEYWORDS: technogenic systems, threats, vulnerabilities, risk assessment, decision making, control of hierarchical systems.

NOMENCLATURE

α_{risk} is an assessment of the risk level;

α_d is an acceptable risk level;

KIA_i is a crisis information agent;

F_i are attack factors;

SV_i is a technogenic system (TS);

Π_i are resource flows;

$\{x_i\}$ is a vector of possible alternatives on the set X of the target space partitioning;

ω_i are external negative factors from the set Ω ;

f is a function of the relationship between decision x and consequence y;

$StratU$ is a control strategy;

R_i are control system resources;

$V(x_i, \omega)$ is a selected alternative for the space partitioning of the system states;

T_m is an interval of the threat;

D_i is an event in the security system, situation;

τ_i is a time of the emergency event;

C_i is a consequence of an emergency event;

$Sit\Pi S$ is a situation in the space of states;

DOI 10.15588/1607-3274-2023-1-14

$\text{Resurs}(TO)$ is a resource of the technological object under the impact of external threat factors;

R_d is a permissible resource value under normal conditions;

$Opt(U/S_i)$ is an optimal control strategy;

V_i are losses upon successful completion of the attack;

$A(f_i)$ is an activity of the factor action on the aggregate structure and control system;

P_i is a probability of the event occurrence;

N_{di}^{f} is a consequence of the influencing factor f_i;

V_{ni}^{f} is a significance of the consequences after the effect of the influencing factor f_i;

$\text{U}(W)$ is a utility function;

Sh_W is a scale of the utility function with the values interval I;

K_i is a mechanisms and requirements for information confidentiality;

$\{Z_i\}$ are types of threats;

$\{Va_i\}$ are loss of information authenticity;

$r(\Pi\alpha_{risk})$ is a flow of cognitive risks;

$\Pi\mu(\alpha_{risk})$ are errors of the personnel;

$\alpha_{risk\,opt}$ is an optimal risk value, which does not exceed the permissible value.

INTRODUCTION

The functioning of any technogenic system in the environment is vulnerable to a variety of interdependent negative factors, independent disturbances and threats that can lead to crisis situations, accidents and catastrophes, if preventive measures to assess the accident risk are not developed and decision-making procedures are not established for control under active informational and cognitive threats. Usually, such procedures and means of counteracting negative factors are provided at the beginning of the design of the protection system and are described in the form of provisions in the security policy of any organization with a hierarchical control system. However, there are negative factors and threats that may arise in the process of the system functioning, which also require the use of a probability approach to determine the risks associated with the action of active threats. Therefore, an important task of the research in the protection system is and will always be the analysis of risk flows, which together form a complex model for assessing the control failure risk for technogenic systems.

If one proceeds from the system concept of assessing the situation in local, district, regional infrastructures, it can be concluded that they were not ready for aggressive attacks on their structure and control process, because they were based on the concept of terminal stability. The action of informational and infrastructural attacks of an aggressive type led to their collapse and the emergence of emergency situations with a high level of accident risk.

The object of the research is the process of functioning of complex systems with a hierarchical structure, in which automated document management systems with a high level of data flow protection for decision-making are used to provide the information quality control of technological processes.

The subjects of the research are the methods and means of constructing an information protection system to ensure the reliable functioning of automated document management systems and making targeted decisions in hierarchical structures with minimal risk of exposure to external threats and attacks.

The goal of this work is to develop a complex model for assessing the risk of the document management system failure as part of a hierarchical production system under active threats.

1 PROBLEM STATEMENT

To achieve the goal of the scientific research, it is necessary to solve the following tasks:

– for the first time, to develop a cause-and-effect diagram of the event formation during the active action of threat factors and attacks, to form the interpretation of risk in a technogenic system in the space of states as a change in the trajectory in the system transitions to the limit functioning mode;

– for the first time, to construct a category diagram of the structure of risk generation under the threat factors and a system-category diagram of interaction in the system *risk ↔ emergency-active nature*;

– for the first time, to develop a system-category scheme of risk formation in the conditions of active threat factors and a cognitive diagram for assessing losses in the event of a risk situation arising from incorrect actions of personnel;

– to test and verify the suggested complex model for assessing the risk of the document management system failure as part of a hierarchical production system for the example of risk assessment of printing productions, as well as to offer a system-category interaction diagram in the game *active factor ↔ accident risk*.

Problem setting is formulated as follows. Let one have some research object SV_i in the input, which is assessed by many indicators depending on the control strategy $StratU$ and security policy. The output may deviate from the control target due to the set of threats $\{Z_i\}$ and the attack factors F_i, which these threats use. As a result of the construction of category diagrams of risk formation in the space of system states under the threat factors in the time interval T_m, it is possible to assess the amount of losses in the risk situations and in the event of incorrect actions of the personnel, the level of which can, for example, be represented by using the models of utility functions for risk assessment $\alpha_{risk} = \{\alpha_{r1}(F_1), \ldots, \alpha_{rn}(F_n)\}$ from the interval [0; 1]. Moreover, the indicators $\alpha_{ri}(F_i)$

DOI 10.15588/1607-3274-2023-1-14

can represent the whole system of criteria and models, on the basis of which one aggregated assessment $\alpha_{risk\,opt}$ on the scale of the utility function Sh_W is derived for each factor of threats and attacks F_i, which is equated to the acceptable risk level α_d.

In addition to quantitative assessments, the reasoning of experts analysing the object is used for the research object. For this, on the basis of experience and knowledge about the research object SV_i, a group of experts (or an expert) analyses it, draws conclusions and assigns one linguistic assessment to each indicator α_{risk}, from the set $r(\Pi\alpha_{risk}) = \left\{F_i; Z_i; KIA_i; Va_i; \mu\left(\Pi\alpha_{risk}\right)\right\}$.

Thus, for a complex assessment of the risk level for a technogenic system, it is necessary to conduct an analysis of the attack factors, multiple threats, loss of authenticity of the control information and possible errors of the personnel, which lead to risk situations and deviations of the system from target orientation. On the basis of the presented input data, for the research object SV_i, it is necessary to derive the initial aggregate assessment of the risk level in the process of the threats impact on the technogenic system $\alpha_{risk} \in [0;1]$. Analysing the value of the assessment α_{risk} and equating it to the permissible values α_d established at the design stage and prescribed in the security policy SV_i, it is possible to adjust the level of its protection by implementing optimal countermeasures.

2 REVIEW OF THE LITERATURE

Analysis of the problem of the emergency and risk situations occurrence, under active threats and attacks, shows the importance of constructing models of attack penetration channels and methods of action on system nodes. In the work of A. M. Shurygin [1], the use of statistical methods for forecasting risk situations and risks assessing is substantiated; the basic concepts, essence, objectives and methods of information protection and the organization of printing productions are revealed in the educational manuals of Vietnamese scientists [2, 3]; in the publications dedicated to the printing industry, the production of securities [4, 5], the peculiarities of the control of printing production and the protection of printing products are considered; scientific publications are devoted to various thorough means of information protection: by Schneier Bruce [6] on applied cryptography, by Mykhailo Sikorsky, and others [7] on analysis of malicious software; the work of L. H. Koval and other scientists [8] is on the analysis of biometric identification methods. With the help of the above-mentioned works, the methods and means of printing production protection are developed, also using the normative legal framework of the Laws of Ukraine [9], as well as the methods of software and hardware protection of network technologies [10], mobile communication devices [11].

In the work [12], modern concepts of information protection against information attacks and system threats are substantiated; the authority control in information security systems, in particular, new approaches to the protection of printing companies, is discussed in the monograph [13].

In [14], information technologies for controlling complex hierarchical systems under threats and information attacks are studied. The concept of risk assessment is formed on the basis of determining the probability and frequency of threats and vulnerabilities for the company assets. The scientific article [15] describes an expert model for assessing risks and security incidents of airport network and information systems, based on intellectual analysis of knowledge using the apparatus of fuzzy sets. Nevertheless, the model is not able to assess the system impact on the process of the functioning system control. The document [16] analyses the concept of risk and safety of subway passengers in cases of malicious technogenic incidents. As a result, the importance of protecting passengers in terms of increasing safety and avoiding dangerous conditions is proven, using the example of the Athens metro system. These studies reveal the essence of hierarchical systems and their vulnerability to technogenic disasters under the external attacks and internal threats impact.

Modern developed methods of analysis of general industrial control systems of hierarchical technogenic structures are presented in the works of foreign scientists [17, 18], and they are given in [19, 20] specifically for complex systems.

The paper [21] presents the application of an object-oriented Bayesian network for scenario risk assessment. A model of probability coverage of key factors influencing accidents in fragmented structures is developed. In the studies [22], a model-based methodology for hybrid control of risk assessment of reliability, availability, maintainability, and safety for critically important systems is proposed. As a result, a method of cyber security risk analysis for industrial control systems is created. Agrawal et al. [23] define the ontology to represent the ISO/IEC 27,005, 2018 standards, with the aim of providing a step-by-step understanding of the meaning of security concepts and their relationships. For example, cyber security ontologies are developed by Arbanas & Čubrilo [24], who are able to construct 52 security ontologies. Researchers such as Blanco et al. [25] considered 31 security ontologies. Both studies group the security ontologies into three categories: general, specific, and theoretical.

Two popular risk assessment methods approved for the nuclear sphere use probability risk assessment [26, 27], and others use dynamic Bayesian networks [28, 29].

In the works of J. Rabcan and others [30, 31], the problem of developing a new algorithm with the application of a fuzzy classifier for signal classification is proposed. The results can be used to automate the process of constructing recognition models using precedents.

Nevertheless, a thorough systematic analysis of terminal risks in technogenic systems under the active threats of resource, information and cognitive types based on category models of influence channels on the control process has not been carried out to date.

DOI 10.15588/1607-3274-2023-1-14

In view of all the above-mentioned facts, it has been decided to carry out an innovative study on the development of a complex model for assessing the risk of the document management system failure as part of a hierarchical production system under the active threats impact.

3 MATERIALS AND METHODS

To analyse risks in technogenic systems and construct schemes and methods for their minimization and control, it is necessary to apply a risk analysis methodology based on the following components:

– the source of risk factors (activity, power, channels);

– the scenario of active actions and the factors impact on the system functioning process (structural, resource, information failure);

– the analysis of the results of the factors effects on the system;

– the structure of the intrusion zone of the active system, which allows the action of an intelligent threat agent through unidentified channels;

– active agents that form the means of the function and structure collapse of the technogenic hierarchical system at the physical level and errors in projects.

The source of risk is related to the consequences of active actions through the scenario – the chain of events of risk implementation in the system under certain conditions, which leads to negative consequences and accidents (Fig. 1).

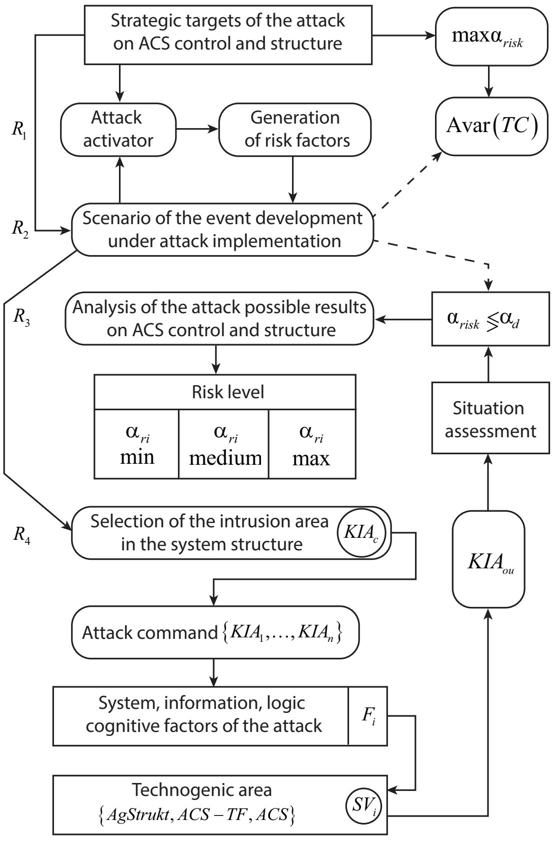
Strategic targets of the attack on ACS control and structure
$\max\alpha_{risk}$
R_1
Attack activator
Generation of risk factors
$\mathrm{Avar}(TC)$
R_2
Scenario of the event development under attack implementation
R_3
Analysis of the attack possible results on ACS control and structure
$\alpha_{risk} \lesseqgtr \alpha_d$
Risk level
α_{ri} min
α_{ri} medium
α_{ri} max
Situation assessment
R_4
Selection of the intrusion area in the system structure
KIA_c
KIA_{ou}
Attack command $\{KIA_1,\dots,KIA_n\}$
System, information, logic cognitive factors of the attack
F_i
Technogenic area
$\{AgStrukt, ACS-TF, ACS\}$
SV_i

Figure 1 – Informational and cognitive map of the system intrusion process

Chains, paths and directions of connections are actually scenarios of the development of a dangerous situation from the point of view of different positions. They describe the scenarios of events that can happen to the system under the action of active factors generated by the source of risks – an active agent, an attacking system, a hidden internal crisis agent, errors of managerial personnel when making decisions.

With the action of active obstacles, cognitive and system factors at the operational and strategic levels of the control hierarchy, due to incorrect decisions and information disorientation, emergency situations and risks of loss of system functions and its target-orientation arise (Fig. 2).

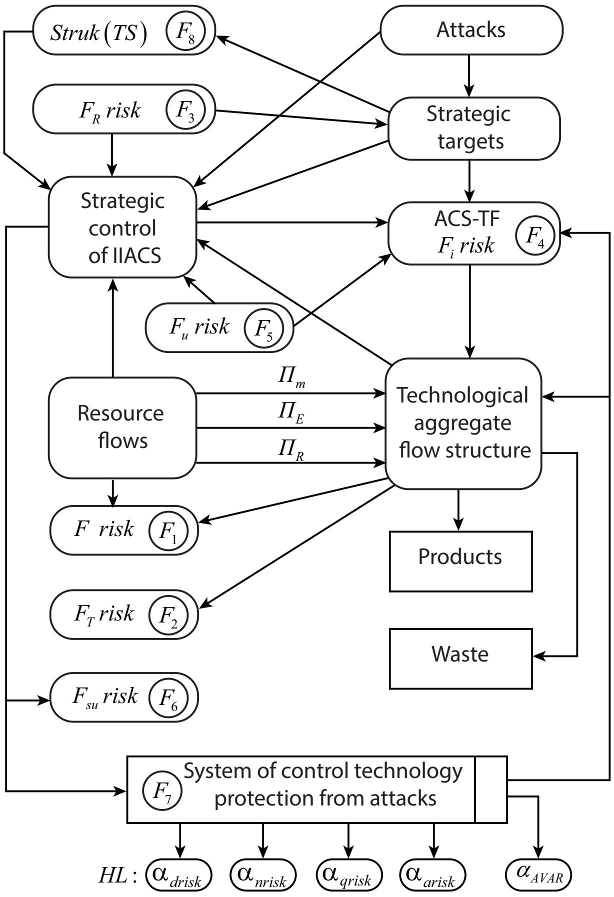

Figure 2 – Category diagram of the formation of hybrid complexes of active risks under the attack factors flow

Here are the schemes for forming a set of risks:

1. Physical risks – physical loss of resources during the system operation, collapse of structures, blocks, aggregates, nodes;

2. Technogenic risks – failure of systems, networks, computers, communications, DoS attacks and threatening destructive actions, power supply failures;

3. Position and cognitive risks – non-compliance with the criteria, regarding the position and abilities of the person, which leads to wrong decisions;

DOI 10.15588/1607-3274-2023-1-14

4. Information risks – loss of data, unauthorized access to ports, terminals, cryptosystems, attacks on databases and information security systems;

5. Management risks – access to decision-making systems, analysis, control, forgery of powers, disorientation of personnel;

6. General organizational risks – conflicts, personnel risks, erroneous setting of targets, inadequacy of situations perception in the control system, inadequacy of strategic targets, sabotage;

7. Risks of violation of the system security level – associated with attacks on the existing levels of the control system, selection and processing of data and decisions;

8. System risks – associated with possible errors when selecting a system concept (targets, structure, dynamics, data processing, control strategies) – by control and operational, project staff.

The level of risk (permissible, sufficient, limit, warning, emergency) is the basis of the classification of both system functioning modes and the assessment of the reliability of the functioning of aggregates, blocks, and control processes in complex integrated hierarchical systems.

The risk of control failure will be analysed in conditions of stochastic uncertainty of the situation under the action of active factors in the space of system states and the target of the control system.

Let one have $\{x_i\}$ – a vector of possible alternatives on an admissible set X of the space partitioning of targets (modes, states).

A rational selection is made according to the consequences that the control action leads to under the factors impact $\omega_i \in \Omega$ at the moment t_i.

The connection between the decision f regarding x and the consequence y is determined by:

$$\exists Strat\left(u/f\right): y = f\left(x, \omega, t_i\right),$$

$$f : \left(X \times \Omega \times T\right) \to Y \to \left\langle f_{onm} \in F \right\rangle,$$

where $\left\{ f\left(x, \omega\right) / t_i \right\}$ – is the function that characterizes (costs-spending); $f : \left(X \times \Omega\right) \to Y$ – is the model of the decision-making process; $y = f\left(x_i \,|_{i=1}^{n}, \omega\right)$ – defines the process of calculating the consequences of the stochastic factor on x_i.

The two-stage decision-making process, under the influencing factor, has the following structure related to the cause-and-effect representation: [1]

1. The decision is made for the first move according to the alternative $x_i \in X$, then random factors are implemented $\omega_i \in \Omega$ ($AF_i \to \tau_i \to D_i \to Sit\Pi S$).

2. The decision is made $y = Y\left(x_i, \omega_i\right)$, which corrects x_i ($\exists StratU, U : x \to y$).

Implementation costs x_i will be $f_1\left(x_i\right)$, and for the implementation $y = f_2\left(x, y, \omega\right)$, thus, if:

$$\exists W\left(\text{Resurs}\left(TO\right) > R_d\right) \Rightarrow \exists Strat\left(U / f_1, f_2\right):$$

$$: \left\langle f\left(x_i, \omega\right) = \begin{cases} f_1\left(x_i\right), \\ f_2\left(x^*, y\left(x, \omega\right), \omega\right) \end{cases} \right\rangle \to \left\langle Opt\left(U/S_i\right)\right\rangle.$$

From the above, it is possible to construct loss functions according to the risk level of control selection on the terminal decision-making cycle for active target-oriented control. At the same time, the level of losses under decision-making risk may depend on the selection of strategies:

1. $F_1\left(x\right) = f\left(x_i, \omega^*\right)$ – are normalized losses of resources, products;

2. $F_2\left(x\right) = \max f\left(x, \omega\right)$ – are the highest losses of the system type;

3. $F_3\left(x\right) = \overset{\omega_i \in \Omega}{\mathrm{M}} f\left(x_i, \omega\right) = f\left(x, \omega\right) P\left(d\omega\right)$ – is the function of the probable average risk under the action of active threats flows;

4. $\begin{matrix} F_4\left(x\right) = P\left\{ f\left(x_i, \omega\right) \le f\left(x, \omega\right) \int P\left(d\omega\right)\right\}: \\ :\left(\omega \,|\, f\left(x, \omega\right) \le c\right) \end{matrix}$ – is the probability of losses under active threats that create an emergency situation.

The risk assessment is determined according to the situation and the activation of the threats, i.e.:

$\alpha_{risk}\left(\omega_i \,|\, x_i\right) = f\left(x_i, \omega\right) = F\left(x\right)$ – is determined by the selected alternative on the space partitioning of the system state in the form of a category diagram (Fig. 3).

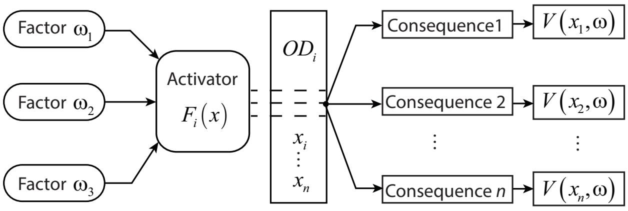

Figure 3 – Category diagram of the structure of risk generation under threat factors

According to the above category diagram, the probability structure of the concept of risk is justified based on the model $\left\langle attack \to consequence \right\rangle$:

$$\forall t_i \in T_m, \left\langle \begin{matrix} \text{if } P_i\left(t_i\right) > 0, \text{ then} \\ Risk = \bigcup_{i=1}^{n}\left(P_i, C_i\right) \Rightarrow \max\left(C_r / V_i\right) \end{matrix} \right\rangle,$$

where P_i – is the event probability; C_i – is its consequence; V_i – are resource losses at C_r; T_m – is the interval of the treat action.

DOI 10.15588/1607-3274-2023-1-14

Then the general risk form for a certain type of active influencing factor is determined according to the formula:

$$\forall t_i \in T_m, V_m^f > 0, P_i > 0: \left\{ \begin{array}{l} Risk = \bigcup_{i=1}^{n} \left(P_i, N_{di}^f, V_{ni}^f\right) \to \min \alpha_v, \\ \text{at } A\left(f_i\right) \to 0 \end{array} \right\},$$

Then the structure of the interaction system $\langle structure \leftrightarrow active\ factors \rangle$ can be presented in the form of a category diagram of threats impact in Fig. 4, 5, 6.

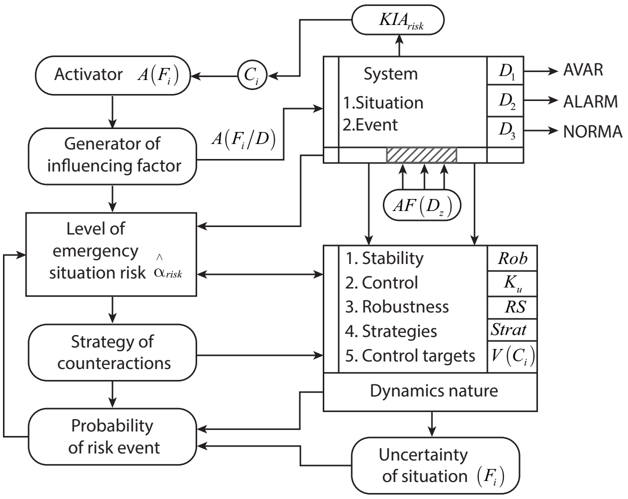

Figure 4 – System-category diagram of interaction in the game $\langle active\ factor \leftrightarrow accident\ risk \rangle$

According to the above analysis of events in the system, which is affected by both control actions and active threats, a set of utility functions of the action of a complex of factors $\left\{F_k \middle|_{k=1,m}\right\}$ is constructed from the selected loss minimization strategies.

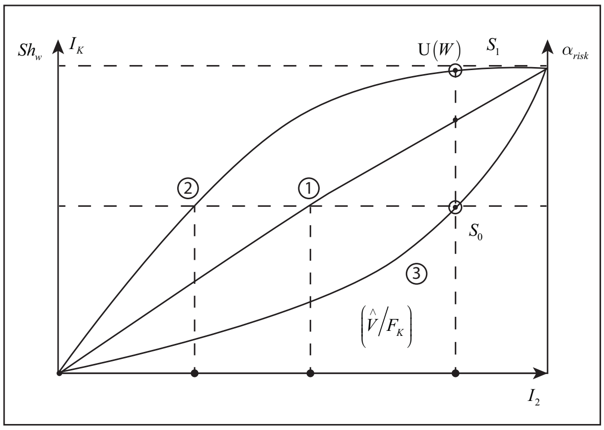

Figure 5 – Graph of the utility function when making decisions

Symbols in Fig. 5: Sh_W – is the scale of the utility function with the value interval I_k; $\mathrm{U}(W)$ – is the Neumann-Morgenstein utility function when forming the decision selection on the set of alternatives; $\left(\hat{W} = \sum_{i=1}^{n} W_i P_i\right)$ – is the expected benefit of the event with the probability of the consequences of the individual selection of the behaviour strategy (target-oriented) in relation to the system, situation $\left(U(W) = P(U \mid S) - (1-p)U(S)\right)$ – i.e. between maximum and minimum $\left(S_1, S_0\right)$.

Graphs of the utility function $\mathrm{U}(W)$ when making decisions of the PMD-KIA (the person making the decision), with the expected benefit $\left(\hat{V}/F_{Ki}\right)$, determines the losses in case of incorrect actions of the operator with different types of behaviour:

1. PMD$_1$ –indifferent to risk (cognitively resistant);
2. PMD – not prone to risk (mentally unstable);
3. PMD$_3$ – prone to risk when making management decisions.

According to the determination of the usefulness level from control actions, under threats, a system-category scheme of the formation of a risk situation in the technogenic hierarchical structure (*TS*) is constructed (Fig. 6).

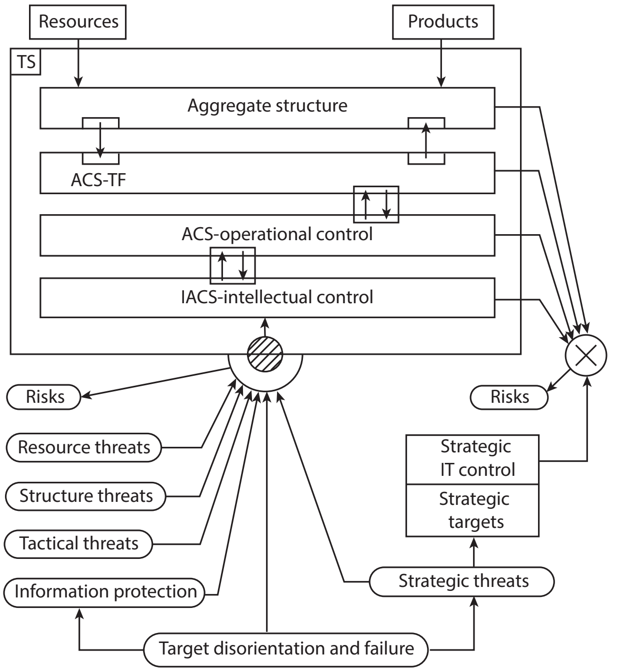

Figure 6 – System-category scheme of risk formation under active threats to the functioning of technogenic hierarchical structure objects

4 EXPERIMENTS

Informational and cognitive threats will be analysed and studied in the automated document management system as part of the hierarchical production system.

The security system is primarily focused on identifying threats and, accordingly, risks of losses for the organization. Such threats include threats to confidentiality, integrity, availability, accountability, authenticity, and reliability of information.

DOI 10.15588/1607-3274-2023-1-14

When assessing the above threats, it is important to directly analyse the security issues with system assets, as this can affect possible threats and, as a result, the selection of protective measures. Usually, such an assessment contains a specific approach to each organization in particular, and also requires the involvement of specialists not only in the field of information protection, but also directly from the organization's specialists, who can assess the system assets, analyse the consequences of damage to these assets and means for restoring the working mode of the system after possible incidents. An information security incident is any unforeseen or undesirable event that can disrupt operations or information security. Information security incidents are: loss of services, equipment or devices; system failures or overloads; user errors; non-compliance with policies or guidelines; violation of physical protection measures; uncontrolled system changes; software failures and failures of technical means; violation of access rules.

Let one consider each of the threats in more detail, analyse the possible consequences of successfully implementing attacks on the system and the necessary countermeasures to reduce them [2–4], and construct a category diagram of the threats actions to the system and control processes (Fig. 7, 8).

Threats to the data privacy about the entire system usually use information access attacks. Threats to privacy can be countered by appropriate privacy and identification services. The methods of such attacks on the information system (*IS*) are usually reduced to three unauthorized actions: spying, eavesdropping and interception.

The mechanisms for ensuring the confidentiality of information in the form of files are presented in Table 1.

Table 1 – File confidentiality mechanisms and requirements for them

Mechanisms for ensuring confidentiality	K_1	Physical security control
	K_2	Access control to the computer files
	K_3	File encryption
File confidentiality requirements	K_4	Identification and authentication
	K_5	Correct setting of the computer system
	K_6	Correct key control when using encryption

Spying (ZA_1) is carried out by accessing unauthorized information and viewing it. If these are paper documents, first of all, it is necessary to ensure their physical protection, preventing third parties from accessing confidential information (security, locks, safes, surveillance and alarm systems, etc.) [12]. If it is an electronic document, then in addition to physical protection and identification of authorized users, it is necessary to implement their authentication methods. At the same time, the following mechanisms of document files confidentiality and requirements for them should be taken into account [13]:

Eavesdropping (ZA_2) can be carried out, for example, by connecting to a line and listening to a telephone conversation. Electromagnetic radiation from sources of information dissemination in *IS* can also be used.

Let one study the threats from information attacks.

If the information is transmitted through an internal or external network, it is possible to intercept it.

In the case of interception, it is important to take into account the fact that an attacker can carry out such an attack, but in order to prevent its further successful development, it is necessary to implement countermeasures to encrypt such information. At the same time, it is necessary to introduce reliable encryption technologies for information flows, or all communication traffic (Fig. 7) [6].

Loss of privacy can lead to the following negative consequences:

– loss of public trust or lowering of the organization's image in the society (VR_1);

– liability before the law, including liability for violation of legislation in the field of data protection (VR_2);

– negative influence on the organization policy (VR_3);

– creating a threat to the safety of the organization's personnel (VR_4);

– financial losses (VR_5).

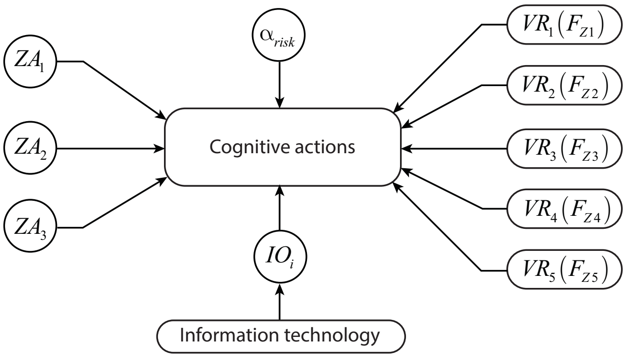

Figure 7 – Cognitive diagram for assessing losses in the risk situation

Symbols in Fig. 7: $\{ZA_i\}$ – are types of threats affecting the system; α_{risk} – is the risk level; IO_i – is a type of the information operation; $\{VR_i\}$ – are losses under the factors impact $\{F_i\}$.

Let one consider informational threats to the data integrity as the basis for errors in the formation of management decisions.

The threat to the information integrity leads to the implementation of attacks on its modification, so all possible negative events that can lead to such incidents should also be analysed (Fig. 8). Such events include the following:

– physical access (ZB_1) to the places of storage of information carriers – it threatens the integrity of the information located on such carriers);

© Sabat V. I., Sikora L. S., Durnyak B. V., Povkhan I. F., Polishchuk V. V., 2023
DOI 10.15588/1607-3274-2023-1-14

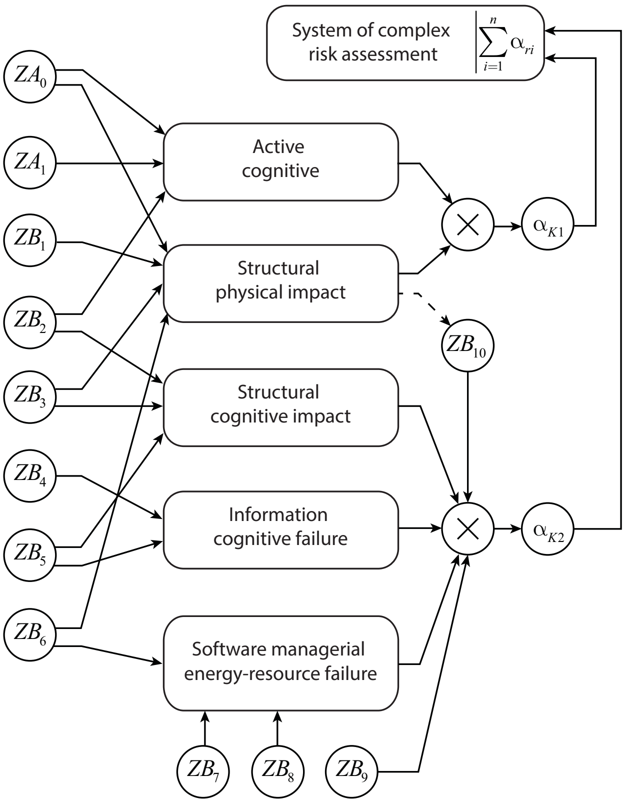
System of complex risk assessment
$\sum_{i=1}^{n} \alpha_{ri}$
ZA_0
ZA_1
ZB_1
ZB_2
ZB_3
ZB_4
ZB_5
ZB_6
Active cognitive
Structural physical impact
Structural cognitive impact
Information cognitive failure
Software managerial energy-resource failure
α_{K1}
α_{K2}
ZB_{10}
ZB_7
ZB_8
ZB_9

Figure 8 – System-category diagram of the impact of a set of threats on the system

– maintenance error (ZB_2) – it occurs if it is carried out irregularly or without compliance with all security policy procedures, then the integrity of the relevant information is at risk;

– malicious code (ZB_3) – it can lead to a violation of integrity, for example, if changes are made to data or files by an unauthorized person who gained access using malicious code, or such changes are made by the code itself [7];

– spoofing a legitimate user ID (ZB_4) – it can be used to bypass authentication and related services and security functions. As a result, integrity problems may arise every time when the information is accessed and modified under the guise of a legitimate user [8];

– sending messages along a wrong or changed route (ZB_5) – it can lead to a violation of integrity, for example, when messages are changed and then transmitted to the original addressee;

– software failure (ZB_6) – it may violate the integrity of data and information that is processed with the help of such software;

– failures in power sources (ZB_7) – (electrical supply and ventilation) – it can cause integrity problems, if such violations are the cause of other malfunctions. For example, power outages can lead to hardware failure, technical malfunctions, or data storage problems. Such problems include technical malfunctions;

– unauthorized access to computers, data, services and applications (ZB_8) – it can become a threat to the information integrity if their unauthorized change is possible [13];

– use of unauthorized programs and data (ZB_9) – it creates a threat to the information integrity in the storage device and during its processing in the system, if these programs and data are used to illegally change information or contain malicious code;

– unauthorized access to the place of storage of information carriers (ZB_{10}) – it may endanger the integrity of this information, because in this case, unauthorized changes to the information recorded on this information carrier are possible.

The integrity service monitors the reliability of information. With the proper level of organization, it gives users confidence that the information is correct and no one has changed it. The integrity service must work together with the identification service to perform a reliable verification of the authenticity of the person, his authenticity to the admission level. Therefore, the integrity service is a “shield” against modification attacks [18].

Loss of integrity can lead to the following:

– making wrong decisions (NR);

– failure in the organization’s commercial operations (NK_o);

– loss of public trust or lowering of the public image of the organization (VD_r) that performs social activities;

– financial losses (VF) from crisis situations and emergencies;

– liability before the law, including liability for violations of legislation in the field of data protection (ZV_Z).

Hybrid threats to the availability of an automated hierarchical control system from attacking agents usually include events that allow attackers to carry out denial-of-service attacks. Among security specialists, such attacks are also called DoS (Denial-of-Service) attacks. The following threats are considered that can lead to the specified attacks [14]:

– destructive actions (ZRD_1) – destructive attacks, which can also be called vandalism;

– physical access (ZRD_2) – to storage locations of information carriers – it threatens the readiness for functioning of storage facilities;

– equipment malfunction (ZRD_3) – connection and failure of communication services;

– maintenance error (ZDp) – it often occurs if maintenance is carried out irregularly or with errors;

– malicious code (ZKd) – it can be used to bypass the authentication and related services and security functions. As a result, this can lead to a loss of accessibility. For example, if data or files are destroyed by a person

© Sabat V. I., Sikora L. S., Durnyak B. V., Povkhan I. F., Polishchuk V. V., 2023
DOI 10.15588/1607-3274-2023-1-14

who gained unauthorized access using malicious code, or the code itself erases files [7];

– spoofing a legitimate user ID (ZIK) – it can be used to bypass the authentication and all related services and security functions. As a result, accessibility problems may arise every time when impersonating a legitimate user makes it possible to delete or destroy information [5];

– incorrect routing (ZMi) or change of message routing [10];

– abuse of resources (ZR), which leads to failures of the network mode.

– natural disasters (ZKS) – impact on the structure and energy supply;

– software failures (ZZp) – it can lead to the unavailability of data and information that is processed with the help of these programs;

– disruptions in supply $(ZNRp)$ – it can lead to availability problems if these disruptions are the cause of other malfunctions. For example, power outages can cause hardware failure, technical malfunctions, or data storage problems. Therefore, it is advisable to provide workplaces with uninterrupted power supply units [12];

– technical malfunctions (ZNI) of nodes, blocks, system structures;

– theft (ZRs) of spare sets for communication and control systems, which leads to an accident;

– traffic overload $(ZNpt)$ – it will reduce system reliability;

– transmission errors (ZNp) – effects of interference on data transmission channels and systems;

– unauthorized access to computers (ZND), data, services and applications – it can become a threat to the information accessibility, if unauthorized destruction of this information is possible;

– use of unauthorized programs and data $(ZNpd)$ – it creates a threat to the information accessibility in the storage device and during processing in the system, if programs and data are used to destroy information or if they contain malicious code;

– unauthorized access to storage locations of information carriers $(ZNdn)$ – it can lead to a risk of information accessibility, since in this case unauthorized destruction of information recorded on these carriers is possible [14].

In accordance with the presented conditions, a diagram of risk formation in the technogenic system is constructed (Fig. 9).

The information accessibility service supports its readiness for work, allows access to computer systems, data stored in these systems, and programs. This service provides the information transfer between two endpoints or computer systems. It is mainly about the information presented in electronic form (but also suitable for ordinary documents).

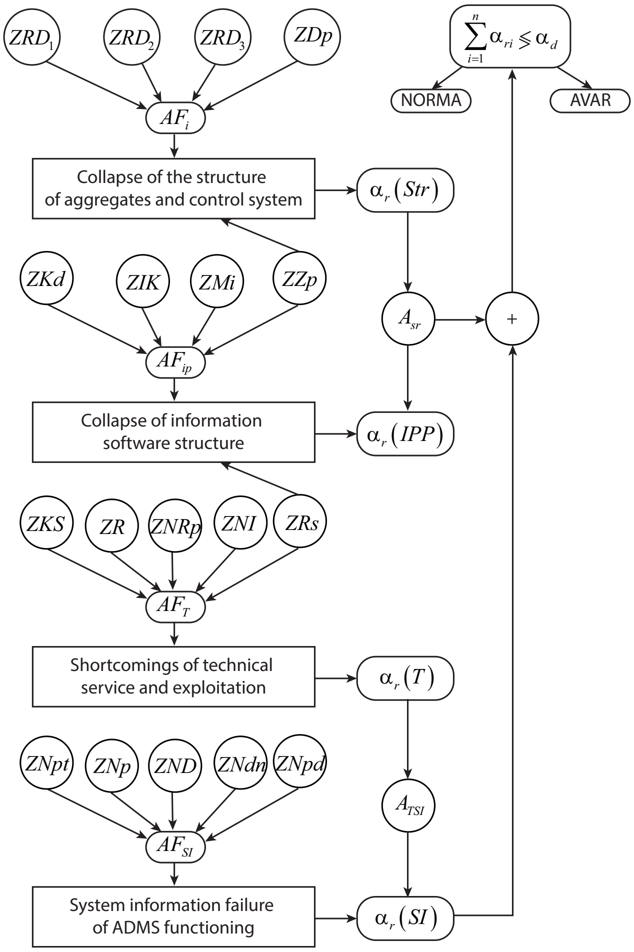
ZRD_1
ZRD_2
ZRD_3
ZDp
$\sum_{i=1}^{n} \alpha_{ri} \lesssim \alpha_d$
NORMA
AVAR
AF_i
Collapse of the structure of aggregates and control system
$\alpha_r(Str)$
ZKd
ZIK
ZMi
ZZp
A_{sr}
+
AF_{ip}
Collapse of information software structure
$\alpha_r(IPP)$
ZKS
ZR
$ZNRp$
ZNI
ZRs
AF_T
Shortcomings of technical service and exploitation
$\alpha_r(T)$
$ZNpt$
ZNp
ZND
$ZNdn$
$ZNpd$
A_{TSI}
AF_{SI}
System information failure of ADMS functioning
$\alpha_r(SI)$

Figure 9 – Diagram of formation of the system accident risk under a complex of threats

Loss of access to data in ADMS and ACS can lead to the following consequences and the action of threat factors:

– making wrong decisions (F_{nr});

– inability to perform important assigned tasks (F_{nc});

– loss of public trust or lowering of the public image of the organization (F_{vd});

– financial losses (F_{vf});

– liability before the law, including liability for violations of legislation in the field of data protection and non-fulfilment of contracts within the established terms (F_{vz});

– significant costs for restoring (F_{vv}) the system structure, communication channels, and software.

Let one consider the threats of accountability for the hierarchy levels of the cyber technogenic system in the implementation of targeted control tasks.

When protecting accountability, any threat that may lead to the performance of actions that are not characteris-

DOI 10.15588/1607-3274-2023-1-14

tic of this object or entity should be taken into account: collective use of accounts; lack of possibility of operational control of actions; imitation of a legitimate user (masquerade); software failure; unauthorized access to the computer, data, services and applications; unsatisfactory authentication. Such threats typically use disclaimer attacks [12, 14].

The loss of accountability, under the factors impact of the system functioning process failure can lead to the following informational and cognitive consequences:

– manipulation of the system by users $\left(ZF_m\right)$;

– deception of personnel at the levels of the system hierarchy (disinformation) $\left(ZF\right)$;

– industrial spying (possibility of attacks) $\left(ZF_p\right)$;

– uncontrolled actions leading to emergency situations $\left(ZF_d\right)$;

– false accusations of incorrect decisions of individuals $\left(ZF_z\right)$;

– liability before the law, including liability for violation of legislation in the field of data protection $\left(ZF_v\right)$.

Let one consider threats to authenticity in the event of data failure and system disorientation.

Trust in authenticity can be undermined by any threat that causes a person, system, or process to doubt that an object is who it claims to be. Examples of the occurrence of such a situation are the change of data without proper control, the origin of unverified or unsupported data (Fig. 10). [14]

Loss of authenticity can lead to the following consequences in the ADMS system:

– deception of the lower levels $\left(Va_{1.1}\right)$ and disorientation of the upper levels of the control hierarchy $\left(Va_{1.2}\right)$;

– use of reliable processes with unreliable data (which can lead to a misleading result) $\left(Va_2\right)$;

– manipulation of the organization from the outside – structure $\left(Va_{3.1}\right)$ and targets $\left(Va_{3.2}\right)$;

– industrial spying regarding target documents $\left(Va_4\right)$;

– false accusations that lead to conflicts in the system $\left(Va_5\right)$;

– liability before the law, including liability for violation of national legislation in the field of data protection $\left(Va_6\right)$.

According to these factors, category diagrams of the formation of hybrid attacks on the information authenticity are developed for each control system (Fig. 10).

Threats of management data inaccuracies are not necessary for assessing the situation and making control decisions.

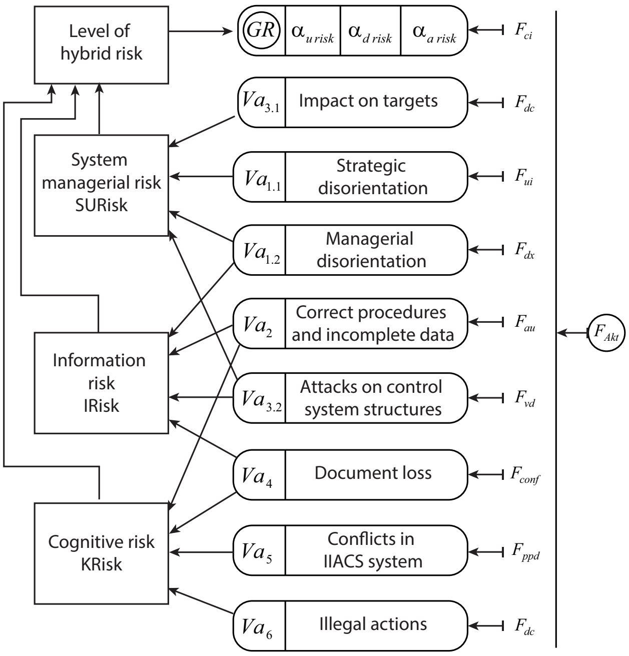
Level of hybrid risk
GR
$\alpha_{u\,risk}$
$\alpha_{d\,risk}$
$\alpha_{a\,risk}$
F_{ci}
System managerial risk SURisk
Information risk IRisk
Cognitive risk KRisk
$Va_{3.1}$ Impact on targets
F_{dc}
$Va_{1.1}$ Strategic disorientation
F_{ui}
$Va_{1.2}$ Managerial disorientation
F_{dx}
Va_2 Correct procedures and incomplete data
F_{au}
F_{Akt}
$Va_{3.2}$ Attacks on control system structures
F_{vd}
Va_4 Document loss
F_{conf}
Va_5 Conflicts in IIACS system
F_{ppd}
Va_6 Illegal actions
F_{dc}

Figure 10 – Category diagrams of the authenticity loss of the control process under internal and external cognitive threats

Any threat that can lead to inconsistent behaviour of systems or processes leads to a decrease in reliability. Examples of such threats are illogical functioning of the system and unreliable suppliers. Decreasing credibility leads to poor customer service and loss of trust.

The loss of reliability can lead to the following consequences in the process of control decision-making under the threat factors:

– deception of the personnel, which leads to a conflict;

– loss of market share due to disorganization;

– decrease in motivation in the work of the organization’s personnel, which leads to the emergence of risk situations during control;

– unreliability of suppliers;

– decrease in customer confidence in the service system;

– liability before the law, including liability for violations of legislation in the field of data protection.

Any attack is implemented through the performance of certain actions that disrupt the performance of the protection system and the automated control system as a whole. For a successful attack, an attacker needs to identify a weak spot in the chain of the protection system and, due to the threats and vulnerabilities of the system, make an illegal intervention in its work. At the same time, the main attention of attackers is aimed at security services, which are focused on countering attacks. Therefore, for the reliable functioning of the security system, an important task is to establish the operation of all its security services and analyse the formation of the characteristics of influencing factors and risk components (Fig. 11).

DOI 10.15588/1607-3274-2023-1-14

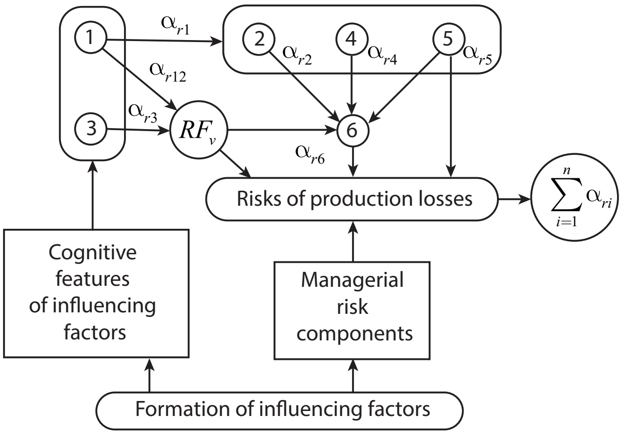
1
3
2
4
5
6
RF_v
α_{r1}
α_{r12}
α_{r3}
α_{r2}
α_{r4}
α_{r5}
α_{r6}
Risks of production losses
$\sum_{i=1}^{n} \alpha_{ri}$
Cognitive features of influencing factors
Managerial risk components
Formation of influencing factors

Figure 11 – A complex model for assessing the system failure risk under active threats

5 RESULTS

The analysis of literary sources and the results of research on the behaviour and knowledge level of operational personnel in energy (KMDandA, ACS) at thermal power plants (coal) was carried out on the basis of a system analysis of cognitive engineering psychology, methods of the theory of knowledge. This became the basis for the development of a table of crisis skills, which provide the possibility of selection and formation of operational anti-crisis management teams in the conditions of active threats and attacks of a complex type (Table 2).

Table 2 – Factors and skills

№	Requirements to the activity	Factor	Coefficient α_r
1.	Information processing of images	FI_V	0.1–0.5
2.	Operational actions	FI_{od}	0.1–0.95
3.	To form images of situations	FI_{syt}	0.1–0.5
4.	Factor of target-oriented actions	FCS_u	0.05–0.95
5.	Factor of action tactics generation	FG_{td}	0.1–0.35
6.	Factor of sensory information perception	FSS_i	0.1–0.25
7.	Factor of skills to implement strategy	FR_{str}	0.1–0.9
8.	Ability to master knowledge	$KFIZ_1$	0.1–0.5
9.	Ability to construct models of objects and event scenarios	$KFIZ_2$	0.05–0.3
10.	System target-orientation when the mode is broken	KIZ_3	0.1–0.95
11.	Formation of images of terminal situations	KIZ_4	0.05–0.25
12.	Analysis of the dynamics of events in the system, control modes	KIZ_5	0.05–0.5
13.	Forecast of the consequences of a person's managerial actions	KIZ_6	0.05–0.95
14.	Genetic features of a person's thinking	IKK_9	0.01–0.3
15.	Motivational and will-power ability to make decisions	IKK_M	0.5–0.95
16.	Cognitive stress resistance	SKI	0.1–0.95
17.	The level of system and professional knowledge of the operator	RSP_zI	0.5–0.9
18.	Ability to apply knowledge in crisis situations (creativity)	$FKSit$	0.1–0.95

Tables of this type ensure the construction of effective tests for the selection of personnel for teams of operational and strategic control levels, which are capable of resisting active threats of a high-risk level.

According to Table 2, a category diagram of influencing factors on the formation of possible cognitive risks – staff errors is constructed (Fig. 12).

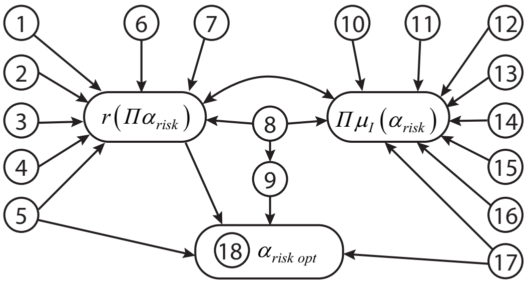

Figure 12 – Category diagram of cognitive risk assessment

6 DISCUSSION

The developed complex model of risk assessment increases the accuracy and objectivity of assessing risk situations, because on the one hand it uses quantitative assessments of the research object (based on data on possible losses in the event of incidents) according to various models and criteria, and on the other hand it uses the experience, knowledge and competencies of experts in the subject area.

The general concept of this approach can be applied not only to companies of the printing industry, but also to any technogenic structures with a hierarchical control structure. Quantitative assessment of losses is presented in the model input obtained according to the analysis of possible threats and vulnerabilities, for example, organizational assets, cognitive characteristics of factors affecting the technogenic structure, taking into account risk coefficients, characteristics of various management components of risk and linguistic considerations of experts-specialists in the field of security and control and decision-making systems. The risks of production losses are formed in the terminal cycle of production and can also be changed under the active threats in the process of production and control. It is necessary to take into account all the threats and vulnerabilities of such technogenic hierarchical systems, and only then it is possible to determine a complex indicator of the system failure risk under active threats. The weight of each constituent indicator of risk can be determined on the basis of the probability approach of the occurrence of one or another event depending on the level of threat to a certain asset, or on the basis of statistical surveys of experts in a specific subject area of research. As a rule, probability approaches coincide with practical statistical results, but unforeseen force majeure circumstances may arise, which, for example, we are currently experiencing during military operations, which destroy all scientific forecasts and conclusions of experts. Assessment and risk analysis of technogenic hierarchical structures was carried out in peacetime, during 2020–2021, for which there are relevant Implementa-

DOI 10.15588/1607-3274-2023-1-14

tion Acts, in particular for the printing production. Based on the received complex assessment of the system malfunction risk, recommendations can be provided for improving the protection system for a certain production and its separate structures, which increases the reliability of the security system.

The developed model of a complex assessment of the system failure risk under active threats does not give a quantitative assessment of the risk, as it determines weak points for the system functioning. In particular, the amount of cognitive risk is difficult to quantify until an incident occurs – a staff or manager error. Therefore, the study substantiated a cognitive diagram for assessing losses in the event of a risk situation with incorrect actions of personnel. The graph of the utility function in decision-making of a decision-maker with expected gains and losses, in case of incorrect actions with different types of behaviour, which affects the cognitive component of the risk level, is presented. In the process of testing with the help of a category diagram *active factor ↔ accident risk*, it is possible to reduce the level of cognitive risk, thanks to the increase in the competencies and skills of the personnel.

Obtaining a quantitative risk assessment for the research object has a number of advantages, namely: it combines quantitative (reliable) assessments with the experience, knowledge, and competencies of experts in the subject area; it is based on the definition of the decision-making utility function; the managerial personnel can be trained and decision-making levels can be adjusted according to the method proposed in the research. The suggested category diagrams and a complex risk assessment model can be used not only in the process of designing protection systems, but also in the process of system operation to solve those problems where there is no data for training and where it is necessary to periodically monitor the security system.

The disadvantages of this approach include the fact that the obtained coefficients of cognitive risk depend on the division of the interval [0,1], and their values depend on the competencies of experts in certain subject areas of research. The training of managerial personnel in the security system also depends on this.

CONCLUSIONS

The paper solves the scientific and applied task of developing a complex model for assessing the risk of system failure under active threats, which, on the one hand, uses quantitative assessments of the object, and on the other hand, takes into account the experience, knowledge and competencies of experts in the relevant subject area.

The scientific novelty of the conducted research is as follows:

– for the first time, a cause-and-effect diagram of the event formation during the active action of threat factors and attacks has been developed;

– the interpretation of risk in a technogenic system in the space of states as a change in the trajectory in the system transitions to the limit functioning mode has been improved;

– for the first time, a category diagram of the structure of risk generation under the impact of threat factors and a system-category diagram of interaction in the system *risk ↔ emergency-active nature* have been constructed;

– for the first time, a system-category scheme of risk formation in the conditions of active threat factors and a cognitive diagram for assessing losses in the event of a risk situation arising from incorrect actions of personnel have been developed;

– the proposed complex model for assessing the risk of the document management system failure as part of a hierarchical production system for the example of risk assessment of printing productions has been tested and verified, and in addition, a system-category interaction diagram in the game *active factor ↔ accident risk* has been suggested.

The practical significance of the obtained results is that the proposed model of complex risk assessment has been tested in the document management system as part of the hierarchical system of printing production and can be used in various technogenic hierarchical systems when solving managerial decision-making tasks, designing and improving protection systems.

The further research of the problem can be seen in the development of software for assessing the risk of system functioning under active threats to technogenic hierarchical structures.

ACKNOWLEDGEMENTS

The work has been performed within the framework of the state-budget research themes of Ukrainian Academy of Printing: “Development of information technologies for the protection of electronic resources in automated document management systems”; Uzhhorod National University: “Methods and means of software engineering for implementing big data analytics processes based on information and technical platforms of electronic science”.

The authors would also like to express their gratitude their partners Aquaflex Plus LLC, Prime-Pak LLC, Sofi Company LLC for the data provided for the implementation of the experimental part of the study.

REFERENCES

1. Shurygin A. M. Applied stochastics: robustness, estimation, forecast. Moscow, Finance and statistics, 2000, 224 p.
2. Kavun S. V., Nosov V. V., Manzhai O. V. Information security. Tutorial. Kharkiv, PH. KhNEU, 2008, 352 p.
3. Veretilnyk T. I., Mysnyk L. D., Mysnyk B. V., Kapitan R. B. Organization of publishing and printing activities: Tutorial Cherkasy. Cherkasy, State Technology University, 2020, 157 p. [Electronic resource] https://er.chdtu.edu.ua/bitstream/ChSTU/3380/1/ORGANIZATION OF%20POLIGRAPHIC%20ACTIVITY.pdf
4. Kovaleva V. V., Samarin Yu. N. Selection of management system for a printing company, *CompuArt. Journal for printers and publisher*s, 2007, No. 11, pp. 61–64.

DOI 10.15588/1607-3274-2023-1-14

5. Honcharov S. V. Financial security of the securities market of Ukraine. Poltava, Poltava State Agrarian Academy, 2019, pp. 40–42.
6. Schneier Bruce. Applied cryptography. Protocols, algorithms, source texts in C language. 2nd edition. Moscow, Triumf, 2002, 816 p.
7. Michael S., Andrew H. Practical Malware Analysis: The Hands – On Guide to Dissecting Malicious Software; translated from English. Chernikov S., St. Petersburg, 2018, 786 p.
8. Koval L. H., Zlepko S. M., Novitskyi H. M., Krekoten E. H. Methods and technologies of biometric identification according to the results of literary sources, *Scientific notes of TNU named after V.I. Vernadskyi*. Vinnytsia, VNTU, 2019, Vol. 30 (69), Part 1, No. 2, pp. 104–112. [Electronic resource] https://www.tech.vernadskyjournals.in.ua/journals/2019/2_2019/part_1/19.pdf.
9. Law of Ukraine "On electronic digital signature", *Bulletin of the Verkhovna Rada*, 2003, No. 36, P. 276.
10. Schneider B. Secrets and Lies: Digital Security in a Networked World. New-York, WCP, 2002, 368 p.
11. Senkivskyi V. M., Petyak Y. F., Kozak R. O., Lytovchenko O. V. Information technology for effective data protection of publishing systems on mobile devices. Lviv, UAP, 2020, 272 p.
12. Bobalo Y. Ya., Horbaty I. V., Bondarev A. P. Information security. Lviv, Lviv Polytechnic University, 2019, 580 p.
13. Durnyak B. V., Sabat V. I., Shvedova L. E. Authority control in information protection systems. Lviv, UAP, 2016, 148 p.
14. Sabat V. Sikora L., Durnyak B., Lysa N., Fedevych O. Information technologies 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. https://ceur-ws.org/Vol-3156/paper23.pdf
15. Kelemen M., Polishchuk V., Gavurová B., Andoga R., Szabo S., Yang W., Christodoulakis J., Gera M., Kozuba J., Kaľavský P., Antoško M. Educational Model for Evaluation of Airport NIS Security for Safe and Sustainable Air Transport. Sustainability, 2020, 12, 6352. https://doi.org/10.3390/su12166352.
16. Milioti Christina, Kepaptsoglou Konstantinos, Deloukas Alexandros, Apostolopoulou Efthymia Valuation of manmade incident risk perception in public transport: The case of the Athens metro, *International Journal of Transportation Science and Technology,* 2022, Vol. 11, pp. 578–588. https://doi.org/10.1016/j.ijtst.2021.07.003.
17. Sicard F., Zamai É., Flaus J. M. An approach based on behavioral models and critical states distance notion for improving cybersecurity of industrial control systems, *Reliab Eng Syst Saf,* 2019, Vol. 188, pp. 584–603. 10.1016/J.RESS.2019.03.020
18. Cormier A., Ng C. Integrating cybersecurity in hazard and risk analyses, *J Loss Prev Process Ind,* 2020, Vol. 64. Article 104044, 10.1016/j.jlp.2020.104044
19. Schmittner C., Gruber T., Puschner P., Schoitsch E. Security application of Failure Mode and Effect Analysis (FMEA), *Computer safety, reliability, and security*. Springer International Publishing, Cham, 2014, pp. 310–325.
20. Vessels L., Heffner K., Johnson D. Cybersecurity risk assessment for space systems, *2019 IEEE Space Comput Conf. (SCC),* 2019, pp . 11–19. 10.1109/SpaceComp.2019.00006
21. Domeh Vindex, Obeng Francis, Khan Faisal, Bose Neil, Sanli Elizabeth Risk analysis of man overboard scenario in a small fishing vessel, *Ocean Engineering*, 2021, Vol. 229, Article 108979. https://doi.org/10.1016/j.oceaneng.2021.108979.
22. Alanen Jarmo, Linnosmaa Joonas, Malm Timo, Papakonstantinou Nikolaos, Ahonen Toni, Heikkilä Eetu, Tiusanen Risto Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems, *Reliability Engineering & System Safety*, 2022, Vol. 220, Article 108270. https://doi.org/10.1016/j.ress.2021.108270.
23. Agrawal V. A. Comparative study on information security risk analysis methods, *J Comput (Taipei)*, 2017, pp. 57–67. 10.17706/jcp.12.1.57-67
24. Arbanas K., Čubrilo M. Ontology in information security, *J Inf Org Sci,* 2015, Vol. 39, pp. 107–136.
25. Blanco C. Lasheras J. , Fernández-Medina E. , Valencia-García R. , Toval A. Basis for an integrated security ontology according to a systematic review of existing proposals, *Comput Stand Interfaces,* 2011, Vol. 33, pp. 372–388.
26. Zhou T., Modarres M., Droguett E. L. Multi-unit nuclear power plant probabilistic risk assessment: a comprehensive survey, *Reliab Eng Syst Saf,* 2021, Vol. 213. Article 107782. 10.1016/J.RESS.2021.107782
27. Modarres M., Zhou T., Massoud M. Advances in multi-unit nuclear power plant probabilistic risk assessment, *Reliab Eng Syst Saf,* 2017, Vol. 157, pp. 87–100. 10.1016/J.RESS.2016.08.005
28. Kim J., Shah A.U.A., Kang H.G. Dynamic risk assessment with bayesian network and clustering analysis, *Reliab Eng Syst Saf,* 2020, Vol. 201, Article 106959, 10.1016/J.RESS.2020.106959
29. DeJesus Segarra J., Bensi M., Modarres M. A bayesian network approach for modeling dependent seismic failures in a nuclear power plant probabilistic risk assessment, *Reliab Eng Syst Saf,* 2021, Vol. 213, Article 107678. 10.1016/J.RESS.2021.107678
30. Rabcan J., Levashenko V., Zaitseva E., Kvassay M., Subbotin S. Application of Fuzzy Decision Tree for Signal Classification, *IEEE Transactions on Industrial,* 2019, No. 15(10), pp. 5425–5434. https://doi.org/10.1109/TII.2019.2904845
31. Rabcan J., Levashenko V., Zaitseva E., Kvassay M., Subbotin S. Non-destructive diagnostic of aircraft engine blades by Fuzzy Decision Tree, *Engineering Structures,* 2019, No. 197, P. 109396. https://doi.org/10.1016/j.engstruct.2019.109396

Received 06.01.2023.
Accepted 11.02.2023.

DOI 10.15588/1607-3274-2023-1-14

УДК 004.451.36:681.5

АНАЛІЗ ТЕРМІНАЛЬНИХ ПОТОКІВ РИЗИКІВ У ТЕХНОГЕННИХ СИСТЕМАХ, ЯКІ ВИНИКАЮТЬ В ПРОЦЕСІ ВПЛИВУ ЗАГРОЗ

Сабат В. І. – канд. техн. наук, доцент, доцент кафедри інформаційних мультимедійних технологій Української академії друкарства, Львів, Україна.

Сікора Л. С. – д-р техн. наук, професор, дійсний член Інженерної Академії України, професор кафедри автоматизованих систем управління Інституту комп’ютерних наук та інформаційних технологій, Львів, Україна.

Дурняк Б. В. – д-р. техн. наук, професор, заслужений діяч науки і техніки України, ректор Української академії друкарства, Львів, Україна.

Повхан І.Ф. – д-р техн. наук, професор, декан факультету інформаційних технологій ДВНЗ «Ужгородський національний університет», м. Ужгород, Україна.

Поліщук В.В. – д-р техн. наук, доцент, професор кафедри програмного забезпечення систем ДВНЗ «Ужгородський національний університет», Ужгород, Україна.

АНОТАЦІЯ

Актуальність. Проведено аналіз термінальних потоків ризиків в техногенних системах, які виникають в процесі впливу інформаційних і когнітивних загроз в автоматизованій системі управління та документообігу в складі ієрархічної системи виробництва.

Об’єктом дослідження є процес функціонування складних систем з ієрархічною структурою, в яких для інформаційного забезпечення якісного управління технологічними процесами використовуються автоматизовані системи документообігу з високим рівнем захисту потоків даних для прийняття рішень.

Предметом дослідження є методи та засоби побудови системи захисту інформації для забезпечення надійного функціонування автоматизованих систем документообігу та прийняття цільових рішень в ієрархічних структурах з мінімальним ризиком впливу зовнішніх загроз і атак.

Метою даної роботи є розроблення комплексної моделі оцінки ризику збою системи управління та документообігу в складі ієрархічної системи виробництва при дії активних загроз.

Метод. Вперше обґрунтовано і розроблено причинно-наслідкову діаграму формування події при активній дії факторів загроз і атак, визначено трактування ризику в техногенній системі та представлено ризик у просторі станів як зміну траєкторії при переході системи в граничний режим функціонування. Вперше побудовано категорну діаграму структури породження ризиків при дії факторів загроз та системно-категорну діаграму взаємодії в системі *ризик ↔ аварійно-активний характер*, запропоновано системно-категорну схему формування ризиків в умовах дії активних факторів загроз. Вперше обґрунтовано когнітивну діаграму для оцінки втрат при виникненні ризикової ситуації при некоректних діях персоналу.

Результати. В результаті досліджень побудовано системно-категорну діаграму впливу комплексу загроз на режим і процес функціонування системи, розроблено метод обчислення рівня системної стратегічної безпеки енергоактивних ієрархічних систем в процесі дії атак і загроз та запропоновано комплексну модель оцінки ризику збою функціонування системи при дії активних загроз.

Висновки. При дії активних завад, когнітивних і системних факторів на оперативному та стратегічному рівнях ієрархії управління із-за неправильних рішень та інформаційної дезорієнтації виникають аварійні ситуації та ризики втрати функцій системи і її цілеорієнтованості. Аналіз комплексу ризиків і запропонована категорна діаграма структури породження ризиків при дії факторів загроз, лягли в основу розроблення ймовірніснісної структури поняття ризику на підставі моделі *атака ↔ наслідок,* а також побудови системно-категорної діаграми взаємодії в грі *активний фактор ↔ ризик аварії*. Це, в свою чергу, дало можливість побудови системно-категорної схеми формування термінальних потоків ризиків в техногенних системах, які виникають в процесі впливу загроз. Комплексна модель оцінки ризику збою системи при дії загроз може бути використана для побудови систем захисту для будь-яких ієрархічних структур управління техногенними системами.

КЛЮЧОВІ СЛОВА: техногенні системи, загрози, вразливості, оцінка ризику, прийняття рішень, управління ієрархічними системами.

ЛІТЕРАТУРА

1. Shurygin A. M. Applied stochastics: robustness, estimation, forecast / A. M. Shurygin. – M. : Finance and statistics, 2000. – 224 p.
2. Kavun S. V. Information security. Tutorial / S. V. Kavun, V. V. Nosov, O. V. Manzhai. – Kharkiv : PH. KhNEU, 2008. – 352 p.
3. Organization of publishing and printing activities: Tutorial Cherkasy / [T. I. Veretilnyk, L. D. Mysnyk, B. V. Mysnyk, R. B. Kapitan]. – Cherkasy : State Technology University, 2020. – 157 p. [Electronic resource] https://er.chdtu.edu.ua/bitstream/ChSTU/3380/1/ORGANIZATION OF%20POLIGRAPHIC%20ACTIVITY.pdf
4. Kovaleva V. V. Selection of management system for a printing company / V. V. Kovaleva, Yu. N. Samarin // Compu-Art. Journal for printers and publishers. – 2007. – No. 11. – P. 61–64.
5. Honcharov S. V. Financial security of the securities market of Ukraine / S. V. Honcharov. – Poltava : Poltava State Agrarian Academy, 2019. – P. 40–42.
6. Schneier Bruce. Applied cryptography. Protocols, algorithms, source texts in C language. 2nd edition. – M. : Triumf, 2002. – 816 p.
7. Michael S. Practical Malware Analysis: The Hands – On Guide to Dissecting Malicious Software / S. Michael, H. Andrew ; translated from English. Chernikov S. – St. Petersburg, 2018. – 786 p.
8. Koval L. H. Methods and technologies of biometric identification according to the results of literary sources / [L. H. Koval, S. M. Zlepko, H. M. Novitskyi, E. H. Krekoten] // Scientific notes of TNU named after V. I. Vernadskyi.

DOI 10.15588/1607-3274-2023-1-14

– Vinnytsia : VNTU, 2019. – Vol. 30 (69) – Part 1. – No. 2. – P. 104–112. [Electronic resource] https://www.tech.vernadskyjournals.in.ua/journals/2019/2_2019/part_1/19.pdf.

9. Law of Ukraine “On electronic digital signature” // Bulletin of the Verkhovna Rada, 2003. – No. 36. – P. 276.
10. Schneider B. Secrets and Lies: Digital Security in a Networked World / B. Schneider. – New-York : WCP, 2002. – 368 p.
11. Information technology for effective data protection of publishing systems on mobile devices / [V. M. Senkivskyi, Y. F. Petyak, R. O. Kozak, O. V. Lytovchenko]. – Lviv : UAP, 2020. – 272 p.
12. Bobalo Y. Ya. Information security / Y. Ya. Bobalo, I. V. Horbaty, A. P. Bondarev/ – Lviv : Lviv Polytechnic University, 2019. – 580 p.
13. Durnyak B. V. Authority control in information protection systems / B. V. Durnyak, V. I. Sabat, L. E. Shvedova. – Lviv : UAP, 2016. – 148 p.
14. Information technologies of active control of complex hierarchical systems under threats and information attacks / [V. Sabat, L. Sikora, B. Durnyak et al.] // The 3rd International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS-2022) Khmelnytskyi, Ukraine, May 25–27, 2022. https://ceur-ws.org/Vol-3156/paper23.pdf
15. Kelemen, M. Educational Model for Evaluation of Airport NIS Security for Safe and Sustainable Air Transport. Sustainability / [M. Kelemen, V. Polishchuk, B. Gavurová et al.]. – 2020. – 12. – 6352. https://doi.org/10.3390/su12166352.
16. Valuation of man-made incident risk perception in public transport: The case of the Athens metro / [Christina Milioti, Konstantinos Kepaptsoglou, Alexandros Deloukas, Efthymia Apostolopoulou] // International Journal of Transportation Science and Technology. – 2022. – Vol. 11. – P. 578–588. https://doi.org/10.1016/j.ijtst.2021.07.003.
17. Sicard F. An approach based on behavioral models and critical states distance notion for improving cybersecurity of industrial control systems / F. Sicard, É. Zamai, J. M. Flaus // Reliab Eng Syst Saf, 2019. – Vol. 188. – P. 584–603. 10.1016/J.RESS.2019.03.020
18. Cormier A. Integrating cybersecurity in hazard and risk analyses / A. Cormier, C. Ng. // J Loss Prev Process Ind, 2020. – Vol. 64. – Article 104044, 10.1016/j.jlp.2020.104044
19. Security application of Failure Mode and Effect Analysis (FMEA) / [C. Schmittner, T. Gruber, P. Puschner, E. Schoitsch] // Computer safety, reliability, and security. – Springer International Publishing, Cham, 2014. – P. 310–325.
20. Vessels L. Cybersecurity risk assessment for space systems / K. Heffner, D. Johnson // 2019 IEEE Space Comput Conf. (SCC), 2019. – P. 11–19. 10.1109/SpaceComp.2019.00006
21. Domeh Vindex. Risk analysis of man overboard scenario in a small fishing vessel / [Vindex Domeh, Francis Obeng, Faisal Khan et al.] // Ocean Engineering. – 2021. – Vol. 229. – Article 108979. https://doi.org/10.1016/j.oceaneng.2021.108979.
22. Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems / [Jarmo Alanen, Joonas Linnosmaa, Timo Malm et al.] // Reliability Engineering & System Safety. – 2022. – Vol. 220. – Article 108270. https://doi.org/10.1016/j.ress.2021.108270.
23. Agrawal V. A. Comparative study on information security risk analysis methods / V. A. Agrawal // J Comput (Taipei). – 2017. – P. 57–67. 10.17706/jcp.12.1.57-67
24. Arbanas K. Ontology in information security / K. Arbanas, M. Čubrilo // J Inf Org Sci, 2015. – Vol. 39. – P. 107–136.
25. Basis for an integrated security ontology according to a systematic review of existing proposals / [C. Blanco, J. Lasheras, E. Fernández-Medina et al.] // Comput Stand Interfaces. – 2011. – Vol. 33 – P. 372–388.
26. Zhou T. Multi-unit nuclear power plant probabilistic risk assessment: a comprehensive survey / T. Zhou, M. Modarres, E. L. Droguett // Reliab Eng Syst Saf. – 2021. – Vol. 213. – Article 107782. 10.1016/J.RESS.2021.107782
27. Modarres M. Advances in multi-unit nuclear power plant probabilistic risk assessment / M. Modarres, T. Zhou, M. Massoud // Reliab Eng Syst Saf. – 2017. –Vol. 157. – P. 87–100. 10.1016/J.RESS.2016.08.005
28. Kim J. Dynamic risk assessment with bayesian network and clustering analysis / J. Kim, A.U.A. Shah, H.G. Kang // Reliab Eng Syst Saf. – 2020. – Vol. 201. – Article 106959, 10.1016/J.RESS.2020.106959
29. DeJesus Segarra J. A bayesian network approach for modeling dependent seismic failures in a nuclear power plant probabilistic risk assessment / J. DeJesus Segarra, M. Bensi, M. Modarres // Reliab Eng Syst Saf. – 2021. – Vol. 213 – Article 107678. 10.1016/J.RESS.2021.107678
30. Application of Fuzzy Decision Tree for Signal Classification // [J. Rabcan, V. Levashenko, E. Zaitseva et al.] // IEEE Transactions on Industrial. – 2019. – No. 15(10). – P. 5425–5434. https://doi.org/10.1109/TII.2019.2904845
31. Non-destructive diagnostic of aircraft engine blades by Fuzzy Decision Tree // [Rabcan J., Levashenko V., Zaitseva E. et al.] // Engineering Structures. – 2019. – No. 197. – P. 109396. https://doi.org/10.1016/j.engstruct.2019.109396

DOI 10.15588/1607-3274-2023-1-14