Using semantic analysis of document text in building risk models in the threats system

Volodymyr Sabat[1,*,†], Bohdan Durniak[1,†], Myroslava Kulynych[1,†], Olena Havrylyshyn[1,†] and Pavlo Hibey[1,†]

[1] *Ukrainian Academy of Printing, 19 Pid Holoskom Str., Lviv, 79000, Ukraine*

Abstract

The article proposes a study of the concepts of risk and safety by introducing semantic parameters and using semantic text analysis in automated document management systems to manage complex hierarchical systems. The author analyzes the cause-and-effect relationships of the occurrence of off-design failures in complex technical objects in the process of managing hierarchical technogenic structures, on the basis of which it is proved that it is better to use preventive methods of detecting failures at the stage of their inception for technical objects, which allows avoiding emergencies and interruptions in the system operation. The proposed methods of building risk models for automated document management systems allow for control at all stages of the document life cycle, from their design, use, and archiving, which ensures increased efficiency and reliability of managing complex hierarchical structures.

Keywords[1]

threats, attacks, risk, semantic analysis, hierarchical systems management

1. Introduction

The use of semantic analysis in modeling protection systems and assessing the risk of emergencies allows for the study of the protection system of complex technical objects using text models. The basis of such approaches is the formalization of the process research area when developing a semantic dictionary for words and phrases, describing their interpretive extensions, implementing rules and certain restrictions in the field of interpretation. Each threat that can be used by an attacker to intrude into a security system or a technological object can be described in a semantic dictionary, which allows, based on its interpretive extensions, to perform a semantic analysis of the occurrence of risk situations for technological objects. This approach is especially relevant if automated document management systems are used to manage complex hierarchical structures, where documents are subject to various attacks related to confidentiality, modification and access to information. Given that documents contain information about the controlling actions of entities over the objects of the technological process, any external negative influences can lead to emergencies. The proposed methods for building risk models using information text models allow synthesizing them into the structures

IntelITSIS'2024: 5th International Workshop on Intelligent Information Technologies and Systems of Information Security, March 28, 2024, Khmelnytskyi, Ukraine

* Corresponding author.

† These authors contributed equally.

v_sabat@ukr.net (V. Sabat); bohdan.durnyak@gmail.com (B. Durnyak); kumyr@ukr.net (M. Kulynych) havrylyshynolena@gmail.com (O. Havrylyshyn); pavlo.hibey@gmail.com (P. Hibey)

0000-0001-8130-7837 (V. Sabat); 0000-0003-1526-9005 (B. Durnyak); 0000-0002-9271-7855 (M. Kulynych); 0000-0001-7181-4421 (O. Havrylyshyn); 0009-0008-2034-1060 (P. Hibey)

of automated document management systems to control the risk of emergencies in the hierarchical structure management system.

An analysis of the literature in this area of research shows certain gaps in this area. For example, while many scientific papers and studies in the field of security and management decision-making have been devoted to the development of risk assessment and management models, little attention has been paid to the semantic analysis of Ukrainian-language content in the course of information attacks and risky emergencies. Given the fact that the number of information cyberattacks is growing every day and that during information wars criminals focus on introducing disinformation into information flows, including documents, there is no doubt that the research problem is relevant.

Investigating technological processes in hierarchical automated control systems under active threats and attacks, we can conclude that in addition to targeted attacks on document management systems and documents in particular, cyberattacks are also directed at complex technical objects of strategic importance. With the development of information network technologies, the number of successful attacks is also growing, which requires security professionals to implement new methods and means of protection and move from reactive to preventive actions to prevent external negative intrusions.

Article [11] discusses the problem of detecting DDoS attacks, analyzes their nature and consequences. Based on the analysis of common types of DDoS attacks, new methods for detecting them based on machine learning, artificial neural networks, support vector machines, and decision trees are proposed. In [12], numerous intrusion detection methods are proposed to combat threats to the information security of technical objects, which can be classified into signature-based intrusion detection systems and anomaly-based intrusion detection systems.

Paper [13] proposes new intelligent algorithms that can perform semantic analysis of text documents in a business environment for the Spanish language. The authors propose methods for processing natural and structured text, text mining to find the most relevant terms, and knowledge engineering to create an ontology to measure semantic similarity in business documents. In [14], computational methods for semantic analysis and quantification of the meaning of short scientific texts are investigated. Computational methods of semantic feature extraction are used to analyze the relationships between message texts and "situation representations" for a newly created large collection of scientific texts. The word meanings are represented by a vector of relative information retrieval about subject categories, which provides the basis for a geometric representation of the semantics of texts. Paper [15] presents a new approach of modified semantic relation based keyword extraction technique based on the semantic relation of similarity between two or more terms. This system extracts a certain number of key terms from documents to determine the main meaning of the text. It uses a support vector machine, logistic regression, PAT-tree, and other machine learning methods.

Rick Durrett in his scientific book [1] describes the probabilistic aspects of risk theory with examples and various exercises. Article [16] explores the risk and uncertainty aspect of business models, in particular, identifying 28 groups of risk and uncertainty factors that can be used as the first step in the process of managing the risk of an integrated business model for existing and new iterations. Paper [2] investigates information technologies for controlling the occurrence of emergencies in complex hierarchical systems in the face of threats and information attacks. The risk assessment is based on determining the probability and frequency of threats and vulnerabilities for the assets of printing enterprises.

Modern concepts in the definition of the theory of reliability of a technical object are given in [3], in which reliability is considered by such parameters as the reliability index, the basics of statistics and probability theory, statistical distributions, such as Weibull, and experiment planning. The engineer must be fully aware of the basic concepts required for reliability testing.

From the customer's point of view, reliability depends on the product design and can be explained by two separate concepts: the service life of a technical object and its failure rate. The construction of emergency forecasting models based on studies of natural disasters is presented in [4], which proposes a methodology for assessing the impact of model parameters on the features of forecasting objects. The main components of the methodology include the use of Latin hypercube sampling to vary the values of model parameters; statistical clustering algorithms for object identification; multivariate multiple regression to assess the impact of several model parameters on the distribution (over the forecast area) of object features and methods to reduce the number of hypothesis tests and control the resulting errors. The basics of technical diagnostics are given in reference [5].

The above scientific works laid the foundation for further research on risk management models using semantic text analysis and automated document management systems.

2. Analyzing the concepts of risk and safety in the event of emergencies using semantic analysis of the research area

Elements of semantic text analysis can be implemented to determine the interpretations of the concept of risk when building appropriate models in the protection system, which are based on the use of an automated document management system (ADMS) for managing complex hierarchical objects of man-made infrastructure. After all, any object or process is described in documents that have information about the control actions of objects over subjects, in separate words x_i or phrases φ_i, which, accordingly, have their own interpretation within the limits of the semantic dictionary defined for this area S_C.

The textual description of the concepts of risk $R(t)$ and safety Bz_i consists of components that can be either words or phrases. To build risk models and analyze interpretive extensions of these concepts, it is necessary to introduce certain rules and restrictions that formalize the subject area of research W_i for the technological process in a certain way. Such semantic parameters and restrictions include semantic significance and semantic contradiction. For example, if the semantic significance of two components of S_C is the same in $\omega_i \in W_i \subset S_C$ but has different interpretations, then they must be semantically contradictory. This rule can be written in the form of a ratio:

$$\langle \sigma^S[R(t), Bz_i] > \delta\sigma^S \rangle, \quad (1)$$

where $\delta\sigma^S$ is the threshold of acceptable semantic contradiction S_C. To semantically define the interpretation of risk $j\big(R(t)\big)$ and security levels $j(Bz_i)$, we can enter their correlations in as follows:

$$\big[j\big(R(t)\big) \in S_C\big]\&[j(Bz_i) \in S_C]\&[\sigma^S[R(t), Bz_i] > \delta\sigma^S] \rightarrow \big[j\big(R(t)\big) = \neg j(Bz_i)\big]. \quad (2)$$

Since $R(t)$ and Bz_i contain numerical values, they must be inversely proportional, or $R(t) = \mathrm{f}(\alpha/Bz_i)$. [1]

To ensure effective counteraction in the security management system (SMS) to possible attacks on the information management system (IMS), it is necessary to introduce for S_C the structure of the interpretation system of all components used to ensure the appropriate levels of security and the rules for the use of words and phrases in the design of documents. In particular, to interpret the concept of risk (t_i), there should be a description of the necessary actions for the appropriate security measures from SMS and a description of the events that a certain danger may lead to.

This means that the interpretation of the risk value can be used to derive the interpretation of the consequences that will result from the action of undesirable factors that determine the established risk value. For a complete description of the hazards, it is necessary to analyze all the vulnerabilities of the technological process [2].

2.1 Cause and effect relationships of off-design failures in complex technical facilities

The task of fault diagnosis is a key one for the problems of ensuring the safety of complex technical facilities. The traditional approach to solving this problem is to detect faults based on the analysis of diagnostic features of technical objects. This means that such diagnostic features ζ_{ij} should be known to the diagnostic system [3]. The diagnostic parameter ξ_{ij} differs from the diagnostic feature ζ_{ij} in that it characterizes a malfunction that has already occurred. The fundamental difference between a fault and a fault occurrence is as follows: a fault represents some event that leads to such possible consequences:

- limitation of the functional capabilities of a technical object (TO),
- the development of a malfunction that could lead to an accident or interruption of the maintenance process.

Failure initiation, or its sign, is an event that can only lead to a malfunction of a technical object. This means that by detecting the signs of a fault, if there are means to counteract its development, it becomes possible to avoid the occurrence of a fault during *maintenance*. In addition, counteracting a malfunction at the initial stage of its manifestation is much easier than counteracting an existing malfunction of a technical object, since it may already have changes that affect the functioning of *the maintenance facility*.

There are a number of technical facilities whose hazard level can be quite high. The hazard level of such technical objects can be determined within the framework of the following approaches.

The first approach is to analyze hazardous situations that occurred at the previous stages of the technical facility's operation and to assess the losses that resulted from the relevant situations. It should be noted that the hazard assessment cannot express the required accuracy in arbitrary units in which it is measured. In most cases, with this approach, the assessment of losses is carried out in units of value. At the same time, losses due to the *fact* that the maintenance facility has ceased to function are not taken into account.

The second approach is to model the process of emergency situations and, based on the data of such modeling, calculate possible financial losses, the value of which is considered as a measure of the danger of a technical facility.

Taking into account the above, we can talk about the existence of estimates of the level of danger of the maintenance facility, which will be denoted by the symbol η_i. The value of η_i in some *maintenance facilities* can be qualified as high. In this case, it is advisable to prevent not only the occurrence of malfunctions, but also their inception.

One approach to solving this problem is as follows. It is known that the occurrence of malfunctions, as well as their inception, is determined by certain causes. If these causes are known, they can be described as some factors affecting the *maintenance,* or they can be internal or external processes. Usually, a negative impact on the *maintenance is* possible only if the values of the parameters of these processes take some unacceptable values. If these processes are known, they can be described in the form of a model, and based on its use, it is possible to predict the possibility of a negative impact of the relevant processes on *maintenance*.

In most cases, there is insufficient information about such negative processes in relation to *maintenance,* and in this case it is difficult to form an appropriate model. Therefore, to solve the problem of detecting the negative impact of such processes on *maintenance*, models for predicting changes in parameter values are used. It is natural to assume that in this case, the values of the parameters are analyzed that have not yet reached the values necessary for the initialization of the processes of fault initiation. [4]

There are cases where all the factors that can lead to malfunctions are not yet known. For example, it may not be the lack of data on certain parameters that may adversely affect *maintenance,* but the lack of information about the possibility of their unacceptable changes. In this case, this problem is solved as follows. A more detailed analysis of the technical object's parameters is carried out in order to identify the values that cause possible changes in their values. To detect unacceptable changes, the problem of predicting changes in the values of the negative parameter ξ_{ij}, regardless of the processes of maintenance operation, is solved.

This approach implies the need to conduct research on the entire functional environment of *the maintenance facility*. Since arbitrary additional research or additional analysis is costly, the need for its implementation is determined by the level of security that must be provided for a particular *maintenance facility*.

Diagnosing off-design faults has a number of peculiarities. Non-design malfunctions are understood not only as malfunctions, such as some unacceptable changes in the *maintenance equipment*, but also as unknown causes of such malfunctions. At the same time, the malfunction itself may be known, since the maintenance facility is an artificially created object. [5] In this case, the question arises as to whether it is necessary to search for such causes and, accordingly, to identify non-design faults. The basis for determining the need for such work is an a priori assessment of the hazard level of the relevant *maintenance,* which can be realized through the use of models of the realization of emergency situations at *maintenance*. Such a model describes possible, known *maintenance* accidents and, based on the data obtained, forms the level of *maintenance* hazard. The peculiarity of such a model is that it is supplemented by a model of initialization of the model itself, which may cause the occurrence and development of a malfunction.

We denote the fault model by the abbreviation MN . In general, such a model can be described by Eq [6]:

$$MN = f_i(\xi_{i1}, \dots, \xi_{im}), \tag{3}$$

where ξ_{ij} is the diagnostic parameters, which in turn can be represented by a correlation:

$$[\varphi_i(\xi_{i1}, \dots, \xi_{ik}) \geq d_i\xi_i] \rightarrow [\xi_i = \varphi_i(\xi_{i1}, \dots, \xi_{ik})], \tag{4}$$

where $d_i\xi_i$ is a certain threshold value of the diagnostic parameter ξ_{ij}, after which the corresponding ξ_{ij} initiates the occurrence and development of a fault described by the function in the model *MN*.

MIN Thefault initiation model, which extends the *MN* model, is described by the following relationship:

$$MIN = \left\{ \forall z \forall x \begin{Bmatrix} \exists x_i[P(x_i) \geq dP_i] \vee \left[\exists z_i\left[P_j(z_i) \geq dP_j\right]\right] \vee [\exists x_i \exists z_i[P_k(x_i, z_i)] \geq dP_k] \rightarrow \\ \rightarrow \left[F\left(x_i, z_i, P_i, P_j, P_k\right)\right] \end{Bmatrix} \right\}, \tag{5}$$

where X is a set of internal parameters that describe the process of maintenance operation; Z a set of external parameters acting on *the maintenance facility*; P_i, P_j, P_k - parameters used in the *maintenance* facility management system; dP_i, dP_j, dP_k - threshold values of the control

parameters; F_i - a function describing the condition of occurrence of a non-design fault. The relationship between the models *MN* and *MIN* is described by the relation:

$$\left[\left[F\left(x_i, z_i, P_i, P_j, P_k\right)\right] \geq dF_i\right] \rightarrow [MIN \rightarrow MN], \quad (6)$$

where dF_i is some threshold of the value of the function F_i.

Detection of a non-design fault within the model (*MNN*):

$$MNN = \Phi[MIN, MN], \quad (7)$$

of a non-design fault is as follows. All external and internal parameters are randomly initiated, while their values are randomly selected for the next random set of x_i and z_i, since P_i are known, they are used at each step of *MIN* and, according to relation (6), the conditions for determining F_i are checked. The above relations describe the general scheme of the methodology for forming a model of non-design faults. The way such a model functions requires a more detailed study of the subject area.

To assess the hazard level of *a maintenance facility, a* system of scales is used, which is formed independently of *the maintenance facility*, based on the analysis of possible events in the environment of *the maintenance facility*, occurring at different distances of these events from *the maintenance facility* within the external environment. [7] In this case, the distances of such events are understood not as the traditional notion of the physical distance between *the maintenance facility*, i.e., a physical object and an event, but as a parametric distance, which is not measured by spatial coordinates but is determined by selected parameters that are common to the external environment and the corresponding maintenance facility. For example, if an accident at *a maintenance facility* occurs as a result of a certain malfunction and can lead to losses $B_i > A_i$ where B_i are losses that exceed the regular costs A_i for the operation of *the facility*, then *the facility* will be classified as a hazardous facility U_i, etc. Usually, the value of U_i is determined by the extent of irreversible or irrecoverable changes in the external environment caused by the consequences of relevant accidents. An example of such a measurement scale is the extent of irreversible changes that have occurred in the natural environment.

In general, the problem of detecting off-design faults is solved by solving the following tasks:

- the task of describing and building a model of the occurrence and development of an emergency situation, which is possible within the framework of technological solutions implemented in a particular maintenance facility;
- solving the problem of identifying the technical causes of the activation of the emergency process within the emergency model (MAC) and identifying the relevant technological parameters, changes in which can lead to the appropriate initialization;
- the task of predicting the occurrence of factors related to the external environment of the maintenance facility that may affect the detected parameters that initiate malfunctions that turn into accidents;
- taking measures to create means of counteracting the relevant factors independent of maintenance;
- transition of the maintenance protection system into a security system by introducing participants independent of maintenance into the protection system to ensure the safety of maintenance operation.

2.2 System models of emergency situations

The task of creating an emergency model consists of two stages, which correspond to the creation of emergency situations of two components *MAC*. The first component models the processes that, from the point of view of the principles of operation of *maintenance* subsystems, can switch to the mode of occurrence, development and development of malfunctions into an emergency situation. At the same time, the means to counteract the relevant processes should be implemented for them at all stages of their implementation. This means that if there are countermeasures at the stage of malfunction initiation, they should be implemented and counteracted at the stage of malfunction development, at the stage of accident occurrence and development, as well as at the stage of influence of man-made parameters on the environment or on the external environment of the relevant *maintenance facility*.

The first component of *MAC* includes the fault model *MN* and the corresponding component of initiating the process of functioning of the fault model *MIN*.

The second component *MAC* is a description of the interaction of external factors related to the relevant subsystems, subsystem components, regardless of the adopted declarations, rules or restrictions on the possibility of the relevant factors *to affect the maintenance*. This component considers the means to ensure compliance with the above rules and restrictions. At the same time, the task of this component is to identify technical possibilities for violating the relevant rules, restrictions, or declarations. Within this component, the task of identifying possible external factors that may lead to the initiation of a malfunction and, accordingly, to the initiation of emergency situations in a technical facility is solved.

The third task is to build models for predicting (*MP*) factors that could be identified because of solving the second task. It is clear that the above numbering order of the tasks does not correspond to the chronological sequence of their solution within the *maintenance* safety system. It should be noted that such factors may not be directly related to technological processes (*TP*), or technical facilities. An example of such factors may be those related to maintenance personnel, which in case of their negative impact on *maintenance is commonly referred to as the* human factor. Factors related to natural processes are those that occur in the environment, for example, the impact of natural disasters that can be attributed to force majeure, etc. From the above analysis, it follows that *MP* does not necessarily apply directly to *MRO*.

Fourth task - as a result of the data obtained from the research at *MP*, systems to counteract the factors identified in the second task are formed as part of the solution to the task. Such systems may also be related to *maintenance*. Examples of such modern countermeasure systems are systems for medical monitoring of aircraft pilots before departure, systems for testing and training of operators who manage *maintenance facilities* recognized as high-risk facilities, such as nuclear power plants, etc. [8,9].

In the case where countermeasures are directly related to *maintenance*, examples of such countermeasures against the possibility of a malfunction are systems for carrying out various preventive measures, including *maintenance* testing measures. As part of a safety protection system (*SZ),* such measures are implemented by automatic protection devices and are an integral part of the entire technological process (*TP)*. This means that when technological maintenance, such as preventive diagnostics or replacement of elements that have exhausted their service life, is included in the *SZ,* then without maintenance work, the *TP* itself cannot be continued, regardless of whether its possible continuation is essential. Ensuring such a mode of operation of the *SZ is* possible only if the means of technological maintenance are combined with the means that ensure the *TP in such a* way that technological maintenance is an insurmountable condition of the *TP* itself, or a necessary stage of the *TP* functioning. This can be

realized in different ways. One of the simplest ways is *to* implement mechanisms within the TP that track events in the process of *TP* functioning that correspond to the implementation of technological maintenance. For example, such mechanisms include a counter for *the* period of maintenance operation, after which technological maintenance should be carried out, and its impact on the work within the *maintenance* itself is that the process of implementing the *TP* is impossible without the necessary technological maintenance of *the maintenance*. [10]

The solution to the fifth task, which is to transform *SZ* into a safety system (*SB)*, or transformation $SZ \rightarrow SB$, which is closely related to the previous task. The fact is that the main functions of the means of ensuring the safety of the *maintenance* operation, which are implemented in the *SB,* are not to counteract the malfunctions that occur in order to prevent the development of an accident, but to prevent the possibility of a malfunction. Such preventive measures are addressed by the following approaches:

- checking and ensuring the implementation of all indirect technological processes;
- modification and development of the system of indirect technological processes (NTP) for individual maintenance facilities;
- calculation of the current value of η_i for maintenance;
- development or modification of SZ, depending on the change in the value of η_i;
- modification of SB tools, if the forecasting of η_i determines an increase in its value for maintenance.

The use of *NTP* as a mandatory component of the *TP of* some *MRO* is a direct consequence of the analysis of the value of η_i, which is determined within the *SB* system models and, first of all, the *MAS* model. The implementation of means for *NTP is* carried out independently of the implementation of *TP* processes in the *maintenance facility* and such means are certain structures that are designed and manufactured at the design stages of *the maintenance facility* and, accordingly, *TP*.

In practice, when designing *maintenance operations* that are characterized by a certain set, or at least one of the factors that have high performance, to which they relate:

- energy capacity;
- is the degree of aggressiveness of individual TP components;
- physical parameters of maintenance;
- volumes of consumption of natural resources of the external environment by the respective TP;
- the degree of dependence of the external environment on the volume of the consumed product produced by the TO also determines the TO hazard, which is calculated based on estimates of losses that may result from the unpredictable impact of the above parameters on the TO and, accordingly, on the external environment.

Predictability or unpredictability is determined based on the following provisions.

The first provision sets out the requirements for the design of a maintenance facility that would ensure not only the feasibility of the *TP,* but also the safety of its operation with respect to the above factors. The parameters characterizing the respective *MT* have properties that are determined by the *MT* components to which they relate. These properties include the service life of individual maintenance items, their resistance to the effects of periodic or rarely acting factors, the possibility of which is known for the design period. Obviously, the calculation of

such properties cannot provide the necessary degree of accuracy in their determination Therefore, the main means of providing protection against such factors are diagnostic tools. Their use is also associated with a certain degree of lack of necessary information, which is as follows:

- insufficiently complete information on the relationship between the established diagnostic parameters and changes that may occur in maintenance components due to negative factors;
- insufficient accuracy of data on possible moments of activation of the impact of negative factors on maintenance and, accordingly, on TP;
- Lack of full characterization and complete information about the processes taking place within the TP functioning, which is typical for complex maintenance facilities;
- lack of information about all possible malfunctions that may occur in the maintenance facility and, above all, about possible ways of their manifestation in the process of operation of TP operating in the maintenance facility;
- Since a characteristic feature of complex maintenance facilities is their period of operation, which is quite long relative to the environment, changes may occur in the environment that lead to changes in the assessment of certain parameters related to the maintenance facility and its components, which could not have been foreseen at the design stage of the maintenance facility.

The above factors are taken into account in the design of *maintenance equipment based on the* use of fairly general methods, examples of which include increasing the resource several times relative to its calculated values, the introduction of certain restrictive conditions and declarations regarding the ways of using *maintenance equipment* and ways to implement permissible changes in the environment and a number of other methods, the implementation of which in the process of *maintenance* equipment operation in most cases is assigned to the maintenance personnel, which is an integral component of the entire technological process, which re.

The above factors are of a technical nature and can therefore be taken into account *to* some extent when designing a maintenance facility. Long-term or, as they are commonly called, long-lived *TPs are* characterized by the influence of economic and social factors, which are closely related to each other. It is known that any *TP* functions in order to interact with the external environment and with the external environment as a whole. Such interaction is realized through the use of economic parameters and factors that are defined in the external environment. Changes in economic parameters that affect the interaction of *MRO* with the external environment can lead to the initiation of fundamental changes in *MRO* not only of the economic type, but also directly to changes in *TP* and *MRO* in general. These aspects are not considered in our study.

Based on the above factors that cause the lack of information necessary for the diagnostic system developed at the design stage of *maintenance to be able to* fully solve the problems of timely detection of malfunctions that may occur during *maintenance*, they can be considered as an additional argument for introducing the concept of non-design malfunctions.

The above factors can be considered not only as an argument for the expediency of using the concept of non-design failures, but also as reasons that determine the possibility of their occurrence, which cannot be foreseen at the design stage of the relevant *maintenance facility*. If we assume that the designers declare the impossibility of certain failures within the framework of the conditions of operation of *the maintenance equipment*, the conditions of their

maintenance, and the conditions formed in the environment, it may lead to the fact that failures may occur, the forms of detection of which are not known at the design stage. Therefore, the following cases of their occurrence and the following forms of their manifestation should be considered as non-design failures:

- malfunctions whose forms of manifestation may be known, but their causes are unknown;
- malfunctions whose forms of manifestation are unknown and, therefore, the causes of their occurrence are unknown;
- malfunctions, the forms of manifestation and causes of which are known, but due to the declarations, conditions and requirements for the methods of implementation and maintenance of the relevant TP are impossible.
- A separate category of non-design problems includes the following:
- malfunctions caused by economic factors or reasons, such as lack of funding, which may be due to various external factors;
- malfunctions caused by social factors that may occur in the event of changes of a social nature in the external environment or the external environment of the maintenance facility.

3. Experimental research

Systems for preventing actions caused and initiated by hazards that exist in relation to technological objects are commonly referred to as Intrusion Prevention Systems (*IPS)*. Any dangerous actions are implemented with the help of certain carriers, which can be implemented in the form of program elements or specialized network software tools similar to the regular components of the system. Such disguised carriers of information dangerous to the system are called intrusions [17].

Based on the analysis of the structure of the production infrastructure, the strategy of attacks on the infrastructure and countering attacks, a model of the information and system game of the attacking structure aimed at destroying the infrastructure of a hierarchical automated control system has been developed (Fig. 1).

Notation in Figure 1: $C_i(A)$ - targets of attack; $C_i(D)$ - goals of counteraction, defense; $Rang(\alpha_{risk})$ - risk rank.

The attacking structure, in the form of an external agent of influence, carries out targeted attacks on the decision-making system, resources, and production infrastructure of the automated process control system. The cognitive information technology of counteraction is based on the system of preventive counteraction to intrusions

It solves the problem of preventing and preventing negative actions against the protected system. The following main functions can be distinguished for *IPS*:

- Zd_1 - searching for threats in the system, if it contains a local area network (LAN) and is connected to the global Internet, then identifying vulnerabilities and possible access coordinates to the security system;
- Zd_2 - Detection of anomalies in the local area network. After identifying the causes of such anomalies that can lead to intrusions into the system, the IPS should activate protection and countermeasures against possible intrusions to prevent further development of an attack on the system through its local network;

- Zd_3 - to prevent further intrusions, if the IPS is unable to counter a possible attack, it redirects it to false targets. To do this, IPS can use false models of the target object, or so-called decoys;
- Zd_4 - prevention of intrusions detected in the IDS, but which can be implemented with a certain attack extension. At the same time, the IPS must have the means to counter augmentation attacks described by signatures already known to the security system;
- Zd_5- Identification of unauthorized scanning of local networks and any actions that indicate the initial stage of the attack.

Detecting threats in computer systems is the most common method and is used mainly in relation to the software components of protected local networks by identifying "weaknesses" in the system software.

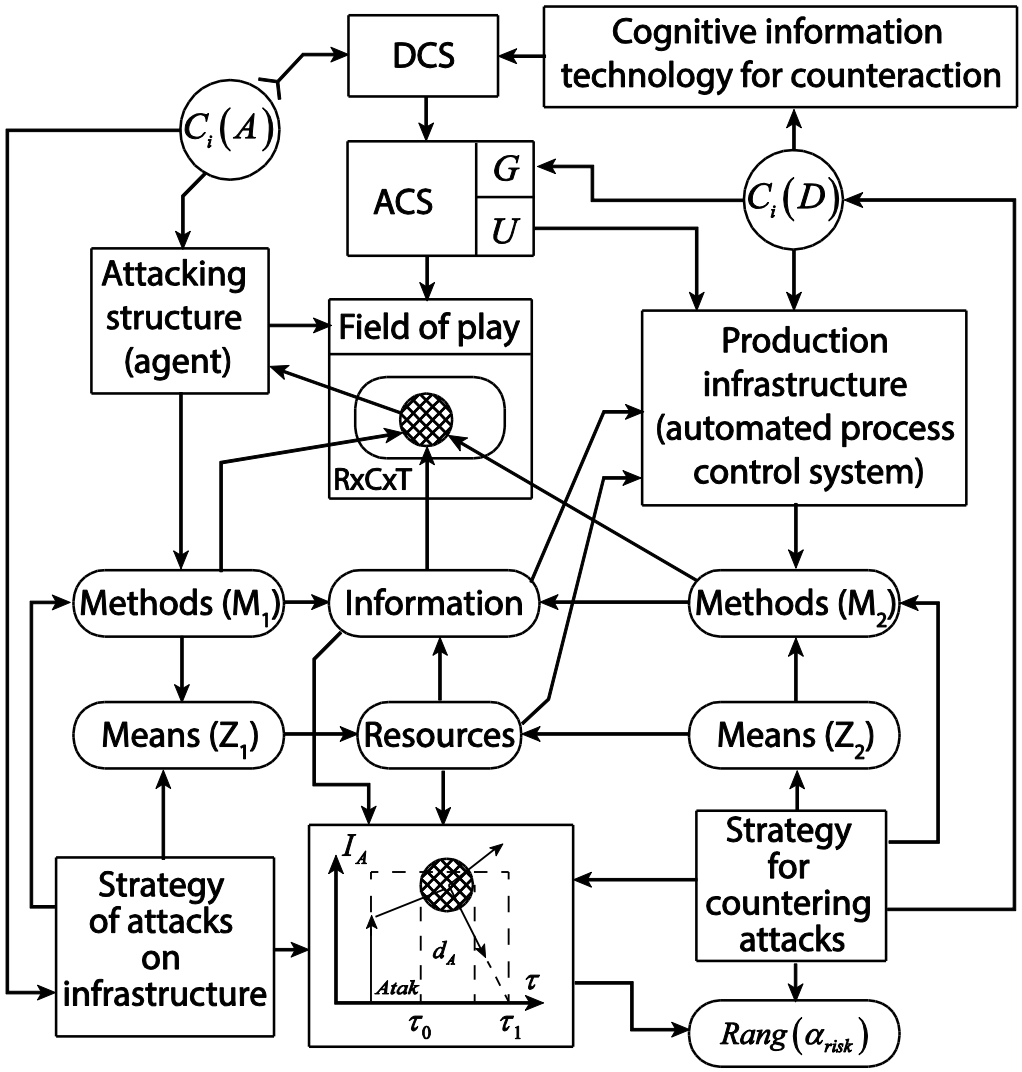

Figure 1: Structural-functional cognitive model of the attacker's game on the control system of the automated process control system of technogenic infrastructure using the concept of cognitive information technology to counter attacks.

When detecting threats, they include a wide range of methods, tools, and technologies:

- SZ_1 - testing systems for software, hardware, and computer networks;
- PZ_2 - network software and its reliability;
- SZ_3 -control of the computer network and its components in the process of operation;
- SZ_4 - use of network analyzers (logic testers, code analyzers, spectrum analyzers).

However, it is not advisable to introduce threat detection tools into the structure of the *IPS* system. In most cases, *IPS* can determine the need to use the appropriate tools from external support resources. Therefore, the *IPS* can have a minimum set of threat detection tools and can replenish it in the course of operation if necessary.

4. Conclusion

Based on the use of semantic parameters and semantic analysis of a certain text area of the interpretation of the protection system and its main parameters with the use of document flow in hierarchical automated control systems, it is possible to model the process of occurrence of non-design problems for technical objects. The interpretation of such concepts as risk and safety in the semantic dictionary makes it possible to predict the consequences that will be caused by the action of undesirable factors, which determines the established amount of risk. For this, it is also necessary to carry out a formal description and analysis of all threats and vulnerabilities for the technological process with the level of their significance for interpreting the risk of emergency situations. Thus, to ensure a certain level of security, based on the amount of risk, you can use semantic parameters and semantic analysis of the research area.

Diagnostic signs of a technical facility that indicate non-design faults are measured through diagnostic parameters during its operation and, if a fault develops, can lead to an accident or irreversible processes in the technical facility. Therefore, it is better to diagnose such negative factors at the stage of malfunctioning in technical facilities. Based on the approaches described in this paper and the proposed models, it is possible to automate this process of detecting non-design faults that lead to malfunctions of a technical object, thereby ensuring the reliability of the system's functioning at the terminal continuous cycle of technical process control.

Transforming a security system into a security system for a technical facility allows you to move from analyzing and counteracting malfunctions that occur in the system as a result of various negative factors, including threats and attacks, to the process of preventing the possibility of malfunctions, i.e., it turns a reactive system for counteracting threats into a preventive system for preventing their detection.

References

[1] R. Durrett. Probability: Theory and Examples. Cambridge University Press. 2019.

[2] V. Sabat, L. Sikora, B. Durnyak, N. Lysa, O. Fedevych, 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, 25–27.05 (2022) 305-318.

[3] W. Seongwoo Modern Definitions in Reliability Engineering. Reliability Design of Mechanical Systems, (2020) 53-99. doi:10.1007/978-981-13-7236-0_3

[4] C. Marzban, C. Jones, N. Li and S. Sandgathe. On the effect of model parameters on forecast objects. Geosci. Model Dev., 11 (2018) 1577-1590. doi:10.5194/gmd-11-1577-2018
[5] Horst Czichos. Handbook of Technical Diagnostics: Fundamentals and Application to Structures and Systems. Springer. 2016.
[6] J. Ren, H. Wang. Mathematical Methods in Data Science. Elsevier; 1st edition. 2023.
[7] J. S. Bendat, A. G. Piersol. Random Data: Analysis & Measurement Procedures. Wiley-Interscience. 2000.
[8] R. K. Baggett, A. L. Stout. Critical Infrastructure Risk Analysis and Management. Handbook of Security Science. Springer, Cham. (2022) 3-32. doi:10.1007/978-3-319-91875-4_1
[9] V. Sabat, B. Durnyak, L. Sikora, V. Polishchuk, Research on the assessment of the risk situations emergence for automated control systems of the metallurgical industry companies. Acta Montanistica Slovaca, (2023) 201-213. doi:10.46544/AMS.v28i1.16
[10] V. J. Sharmila, D. J. Florinabel, A Two-Step Unsupervised Learning Approach to Diagnose Machine Fault Using Big Data. Information Technology and Control 51, 1 (2022) 78-85. doi:10.5755/j01.itc.51.1.29686
[11] M. Chornobuk, V. Dubrovin, L. Deineha, Cybersecurity: research on methods for detecting ddos attacks. International scientific journal «Computer systems and information technologies», 4 (2023) 6-9. doi:10.31891/csit-2023-4-1
[12] A. Khraisat, I. Gondal, P. Vamplew & J. Kamruzzaman, Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity 2, 20 (2019). doi:10.1186/s42400-019-0038-7
[13] R. Rodriguez-Cardosa, F. P. Romero Chicharroa, J. A. Olivas-Varelaa, J. Serrano-Guerrero. A method for the semantic analysis of documents in a business context in Spanish. Procedia Computer Science, 162 (2019) 803-810. doi:10.1016/j.procs.2019.12.053
[14] N. Suzen, A. N. Gorban, J. Levesley & E. M. Mirkes. An Informational Space Based Semantic Analysis for Scientific Texts. Computation and Language, (2022) 81-99. doi:10.48550/arXiv.2205.15696
[15] H. M. M. Hasan, F. Sanyal and D. Chaki, 2018. A Novel Approach to Extract Important Keywords from Documents Applying Latent Semantic Analysis, 10th International Conference on Knowledge and Smart Technology (KST), Chiang Mai, (2018) 117-122. doi:10.1109/KST.2018.8426144
[16] A.-S. Brillinger, Ch. Els, B. Schäfer, B. Bender, Business model risk and uncertainty factors: Toward building and maintaining profitable and sustainable business models. Business Horizons, Volume 63, Issue 1, (2020) 121-130. doi:10.1016/j.bushor.2019.09.009