Jerzy KOROSTIL
MARITIME UNIVERSITY IN SZCZECIN
1-1 Wały Chrobrego St, 70-500 Szczecin

Features of predicting random events and protection of technical objects from their influence

Abstract

The paper presents research results of approaches to solving tasks of predicting occurrence of events that negatively affect technical objects. Among them, super-rare events stand out (events that occur randomly in big time intervals) and analysis of features of predicting them is conducted. Measures of protecting technical objects from negative influence of random events are reviewed, and a method of estimating the prediction accuracy on the basis of using risk concepts is presented.

Keywords: prediction, attack, risk, random event, safety.

1. Introduction

Prediction of random events (Vp_i) is considered reasonable only in case when it is assumed or proved that such events can have a negative influence on a certain technical object or an environment (Sr), or can be used for beneficial purposes in Sr, which is the scope for research [1]. Influence negativity in most cases is declared, and a way of negative influence of Vp_i on Sr is determined. Negativity or positivity of the corresponding influence of Vp_i on Sr is determined by interpretations of interaction of Vp_i with Sr. These interpretations depend on the Sr type, concepts of processes occurring in Sr and depend on objects that form Sr. Let us assume the following conditions that will allow a more constructive approach to the Vp_i prediction tasks.

Condition 1. If, related to Sr, Vp_i can occur, the latter are recognized in Sr.

Condition 2. An influence of Vp_i on Sr is performed by activating a certain process Pr_i in Sr.

Condition 3. Elements of Sr are complex technical objects (CTO_i) and their functioning processes $Pr_i(STO_i)$.

Condition 4. A set of processes Pr_i in Sr is characterized by signs of their positive or negative influence on CTO_i objects.

Condition 5. Prediction is effective if a time interval Δt_i, called a prediction interval, between the moment of obtaining data regarding the prediction result and the moment of occurrence of the predicted event is sufficient to ensure the possibility of using Vp_i^N, or implementation of withstanding the negative influence Vp_i^N on a certain object or a process.

Processes that are activated by events Vp_i are customary to be related to implementing attacks on CTO_i written as At_i. Each At_i or their groups can be correlated to the corresponding dangers Nb_i, that are external for Sr. Let us assume that each event Vp_i activates an attack At_i on CTO_i, which is performed as a certain process Pr_i in an CTO_i object. Let us assume the classification of attacks At_i proposed in [2]. Events of Vp_i^N type will be correlated to attacks of At_i^N type, that lead to occurrence of catastrophic situations $\mathcal{K}a_i$ in the CTO_i objects.

Tasks of prediction of different types of Vp_i have to be reviewed considering the following cases:

- Prediction that foresees occurrence of a certain Vp_i at the time interval $t_i + \Delta t_i$, where t_i is the current time when the prediction result becomes known,
- Prediction of change of parameters in CTO_i, that lead to transition of CTO_i in the catastrophic state,
- Prediction and determination of factors that lead to occurrence of events of Vp_i^N type.

The first case corresponds to the situation when, as a result of predicting Vp_i^N, the time moment $T_i = t_i + \Delta t_i$ is determined when the Vp_i^N event will occur. At that, information regarding the event itself within this approach is assumed on the basis of prior data.

The second case lies in prediction the fact of occurrence of $\mathcal{K}a_i(CTO_i)$ and is implemented on the basis of determining the possible values of CTO_i parameters that characterize the corresponding $\mathcal{K}a_i(CTO_i)$. In order to correlate this prediction type to the time scale of the CTO_i functioning process, it is necessary, on the basis of analysis of the functioning model $MF(CTO_i)$, to determine the time needed for the corresponding parameters of CTO_i during the current functioning to take on the critical values if the corresponding process leads to this. Parameters that characterize $\mathcal{K}a_i(CTO_i)$ are chosen on the basis of data regarding single components of CTO_i and processes that characterize its functioning. Because any processes in CTO are implemented within certain time intervals $\Delta\tau_i$, the intervals Δt_i lie within $\Delta\tau_i$ of single processes $Pr_i(CTO)$. The time during which $Pr_i(CTO)$ are performed is customary to call the real functioning time of Pr_i [3]. Determining the moment of possible occurrence of Vp_i^N, which is T_i, and determining the values of parameters that lead to occurrence of critical situations in CTO, is based on the fact that the corresponding model of a process $MF(Pr_i)$ can function faster than $Pr_i(CTO)$ functions in real time. This means that functioning of a model MF(Pr_i) can be performed at the modeling time $\Delta\tau^M$, while the real functioning time interval of $Pr_i(CTO)$, which is $\Delta\tau^R$, is bigger, or $\Delta\tau^M < \Delta\tau^R$ so the following is true: $\Delta t_i = \Delta\tau^R - \Delta\tau^M$. Unlike the previous case when the prediction model is oriented towards determining the moment T_i of occurrence of Vp_i^N, in this case the corresponding model is a functional prediction model which will be written as $MF(PG_i)$.

In the third case the prediction is formed on the basis of analysis of factors that lead to changes in CTO that can have a catastrophic nature. These factors are closely related to the dangers Nb_i that generate attacks At_i that, in turn, activate in CTO the corresponding processes $Pr_i[At_i(CTO)]$. In this aspect it is assumed that in the Sr environment there is a certain information regarding single Nb_i, information regarding the possible At_i that are generated in Nb_i, and information regarding the possible influence of various At_i on CTO_i objects and their processes. On the basis of this information regarding At_i, Nb_i and ways of influence of At_i on CTO_i, in CTO_i a safety system (SB) is formed that consists of measures of protection and withstanding the negative influence of the corresponding attacks. Because, regarding the known attacks, CTO_i has the SB system, the negative influence can only be performed by attacks of the At_i^N type. In this case, the prediction model is built on the basis of using the possible models of functioning processes Nb_i. This model of prediction of occurrence of random events of different types, including events of a Vp_i^N type, will be written as $M[PG_i(Nb_i)]$. An example of external dangers can be natural dangers such as storms on the water surface, earthquakes, floods and so on. An example of technological dangers can be hacker information systems, processes caused by war events and others [4].

All given approaches for building prediction models, although based on using the various data, allow to consider all external and internal factors leading to a negative influence when acting on a protected object.

2. Features of tasks of ensuring the safe CTO_i functioning

To ensure the safe CTO_i functioning, a necessity arises for determining the necessary degree of protection of CTO_i from possible attacks. Solving of this task is based on estimating the

possibilities of protection measures of CTO_i and estimating the processes that implement this protection. Because we first of all talk about attacks of the At_i^N type and the catastrophic situations $\mathcal{K}a_i$ with CTO_i, we have to consider some features that characterize $\mathcal{K}a_i(STO_i)$.

The first of these features is quite big interval of occurrence of a catastrophe $\mathcal{K}a_i(CTO_i)$ comparing to periods of occurrence of emergency situations caused by the corresponding attacks. Each technical object has one of basic characteristics which is a functioning resource of the corresponding CTO_i, written as ΔTR [5]. The resource parameter is interpreted as a time interval when CTO_i has to function corresponding to the technical requirements. The resource is ensured not only by creating reliable nodes of CTO_i and the object in general, but also by creating components of a safety system $SB_i(CTO_i)$ that solve tasks of detecting and withstanding attacks and consists of the following components: diagnostic system, system of predicting the negative events, attack models and other systems. Let us introduce the following definition.

Definition 1. A catastrophic situation is a situation when the period of occurrence of $\mathcal{K}a_i(CTO_i)$ is comparable to the value of a resource ΔTR_i of the corresponding CTO_i and changes in STO_i that occurs in this case lead to impossibility of continuing the technological process $Pr_i(STO_i)$.

This definition means that the period of occurring of Vp_i^N, the influence of which can be written as the following relation: $Vp_i^N \rightarrow At_i^N \rightarrow \mathcal{K}a_i(CTO_i)$, can be assumed close to $\Delta TR_i(CTO_i)$, which can be written as: $\Delta T_i(\mathcal{K}a_i) \propto \Delta TR_i(CTO_i)$. Thus, prediction catastrophic situations has to be long-term, also, together with other factors during prediction, a resource of an object has to be considered, relating to which predicting of Vp_i^N event is performed. Moments of occurring of Vp_i^N are not necessarily synchronized with moments of depleting of the resource in the corresponding CTO_i. Let us assume that $\Delta TR_k(CTO_i)$ is less than $\Delta T_k(Vp_i^N)$, where $\Delta TR_k(CTO_i)$ is a value of a resource of CTO_i that has not been depleted yet, and $\Delta T_k(Vp_i^N)$ is a certain generalization of an approximate period of occurring of a Vp_i^N event. If the prediction system $S(PG(Vp_i^N))$ will predict the occurrence of a Vp_i^N event after the time Δt_i, the system $SB_i(CTO_i)$ has, during the time Δt_i, to recognize a possible attack At_i^N, where $Vp_i^N \rightarrow At_i^N$, and generate and use the measures of withstanding the corresponding At_i^N.

On the other side, it is not reasonable to predict Vp_i^N that lead to $\mathcal{K}a_i(CTO_i)$ at time moments that correspond to the time period δt_i, which is a fragment of CTO_i functioning that corresponds to the relation:

$$\delta t_i(CTO_i) < \Delta TR_i(CTO_i),$$

This means that a prediction $Vp_i^N \rightarrow \mathcal{K}a_i(CTO_i)$ is reasonable to activate so that the following relation would take place:

$$(t_i = \Delta TR_i - \Delta t_i) \leq \delta t_i.$$

In order to consider long-term predicting $\mathcal{K}a_i$, the corresponding model $M[PG_i(CTO_i)]$ has to consist of the following parts:

1. Modeling of the process of decreasing of resource $\Delta TR_i(CTO_i)$.
2. Defining the time moment t_i when it is reasonable to activate the predicting process.
3. Define the time interval of a prediction Δt_i, for which the following relation would take place:

$$\{\delta t_i[(M(Pr_i(CTO_i))] + \Delta t_i[PG(CTO_i)]\} < \Delta TR_i(CTO_i).$$

The first component corresponds to the functioning period $\delta t_i(CTO_i)$, which is less than $\Delta TR_i(CTO_i)$, so it is not reasonable to predict $\mathcal{K}a_i$.

The second component Δt_i defines the time interval when the prediction $PG_i(CTO_i)$ is performed, and this interval together with the first component has to be greater than $\Delta TR_i(CTO_i)$.

The second feature lies in the fact that it is not always reasonable to implement protection and withstanding measures for all known attacks oriented towards a single type of CTO_i. This is caused by the fact that intensity of various attacks depends on various factors related to features of specific dangers Nb_i and to features of various objects of CTO_i. This leads to the possibility for attacks not of the type At_i^N, but with small intensity, to also cause the occurrence of $\mathcal{K}a_i(CTO_i)$. This is especially vital for objects of CTO_i that are characterized by functioning periodicity, a typical example of which is sea transport. Occurrence time of each event Vp_i is counted from the beginning of the functioning process of CTO_i at a single period of its work, but in prediction models $M(PG_i)$ data and information from all previous functioning stages of CTO_i are considered. Because various intervals of functioning process of CTO_i can be longer or shorter, the prediction interval Δt_i can be longer or shorter, too. The user of CTO_i is only interested in those possible random events and the corresponding attacks that occur during the current interval of CTO_i functioning. If at the current functioning interval of CTO_i an event occurs with not high occurring intensity, it could be the case that there are no foreseen measures in *SB* for detecting an attack activated by this event, although these attacks can also lead to catastrophic situations. This attack will be called a pseudo-unexpected attack. Let us introduce a definition of such an attack.

Definition 2. We will call pseudo-unexpected attacks At_i^P the attacks that are known but have no implemented protection and withstanding measures in *SB* from CTO_i.

The main reason of separation of attacks At_i^P from the class of known attacks At_i is their low intensity in the functioning interval of CTO_i. Because of this, within the system $SB_i \subset CTO_i$ it is necessary to implement measures of predicting events of the type Vp_i^P that activate attacks At_i^P. In general, attacks of the type At_i^P are known. We can deduce that information regarding the danger Nb_i, that corresponds to attacks $At_i^P \subset At_i$, and information regarding the attacks At_i^P themselves in general case is somewhat known. This leads to the possibility to build the corresponding models of predicting the occurrence of events Vp_i^P and the corresponding attacks At_i^P, that are described by the following relation: $M(PG_i^P) = F[D(Nb_i), M(At_i^P)]$, where F is a function that describes the process of synthesis of data about the danger $D(Nb_i)$ and the known model of an attack $M(At_i^P)$.

The third feature of solving tasks of ensuring the functioning safety lies in necessity to consider internal factors of CTO_i that can also lead to the catastrophic events. In general case, internal factors are malfunctions that occur because of various reasons. Among such reasons, external reasons can be named that, when influencing the elements of CTO_i, can lead to malfunctions in the corresponding CTO_i components, and also internal reasons of malfunction occurrence that are caused by depleting the resource of a single node, decrease of reliability measure of a single node, for instance, as a result of its unplanned overload, etc.

The internal reasons in most cases lead to malfunctions in CTO_i. The tasks of detecting malfunctions are performed by diagnostic systems that are the mandatory components of a safety system of CTO_i [6]. The process of malfunction occurrence is quite complex and consists of the following stages:

- A stage of malfunction origination, when the parameters of a certain element are changed,
- A stage of malfunction development, when parameters are changed under the influence of internal factors,
- A stage of malfunction forming, when the malfunction starts to inappropriately influence the value of functional parameters of the process.

If a malfunction has arisen and its development has stopped, then an anomaly appears within nodes of CTO_i that is typically called a threat [7].

If this anomaly is not described in the diagnostic system by a diagnostic parameter, it is not detected by this system. Diagnostic systems are not oriented towards detecting anomalies that do not

lead to disrupting the functioning process of CTO_i, so this anomaly can exist in the CTO_i components for a relatively long time. These threats can be used by dangers to form successful attacks, which is quite widespread in the information systems [8]. Because any Nb_i influences the CTO_i elements using attacks At_i, let us introduce one more attack type that will be called internal attacks At_i^V. Because in this case there is an unknown threat in the form of an anomaly that occurs randomly, the occurrence of an attack At_i^V can be considered a result of its influence on an object of a random event of the type Vp_i^V, that are determined on the basis of using the corresponding prediction model which can be written as follows:

$$M\left(PG_i^V\right) = F[D(Nb_i), M\left(At_i^V\right)].$$

3. Organization of a system of predicting the catastrophic situations

Based on the mentioned features of solving tasks of protecting CTO_i from a negative influence of Vp_i^N, or $Vp_i^N \rightarrow At_i \rightarrow \mathcal{K}a_i(CTO_i)$, we can state that solving the task of predicting the catastrophic situations, with consideration of all factors that cause such an event, is rather difficult. Thus, it is not reasonable to create a complex predicting system that requires a lot of data and a big variety of complex calculations in order to determine the occurrence time and the type of a catastrophic situation in CTO_i that are super-rare events. Let us introduce the following definition.

Definition 3. A super-rare random event Vp_i^{Na} is an event, the occurrence period of which is proportionate to $\Delta TR_i(CTO_i)$ and which causes the occurrence of $\mathcal{K}a_i(CTO_i)$.

We will only consider unexpected events as super-rare, or $Vp_i^{Na} \equiv Vp_i^N$.

A feature of using the result of predicting an event that causes $\mathcal{K}a_i$ lies in the fact that users are not interested in events that can occur in quite a big time interval. This is especially relevant if a resource of CTO_i, that is defined by guaranteed time interval of safe functioning $\Delta TR(CTO_i)$, is much bigger than an interval that is defined by difference between the current moment and the moment of start of the first functioning interval $\Delta TF(CTO_i)$. A user is first of all interested if an event $Vp_i^N \rightarrow \mathcal{K}a_i(CTO_i)$ will occur during the current functioning interval of CTO_i, when the following relation takes place: $\Delta TR(CTO_i) > \Delta TF(CTO_i)$, where ΔTF is the sum of CTO_i functioning intervals that does not exceed $\Delta TR(CTO_i)$, or $\{[\Delta TF(CTO_i) = \sum_{i=1}^{m} \delta t_i(CTO_i)] < [\Delta TR(CTO_i)] \& [\delta t_{m+1}(CTO_i) + \Delta TF(CTO_i)] > \Delta TR(CTO_i)\}$.

With these conditions, it is reasonable to create a system of predicting $\mathcal{K}a_i$ that includes all the necessary components of an environment Sr. A common prediction system has to be implemented as a distributed system that uses data formed by safety systems of all CTO_i that are functioning in the different components of the safety system, that are placed in CTO_i and other systems that are functioning in the environment Sr, that are united with each other on the basis of chosen common parameters and are external to CTO_i. To solve the tasks of predicting super-rare events Vp_i^N that lead to $\mathcal{K}a_i$, a wider choice of data can be used, if we take into consideration that the value of outspent resource in various CTO_i can be different. Thanks to this, it is possible to build prediction models not only on the basis of input data used in models based on using analytic descriptions of prediction models, but also on the basis of prediction models based on using analogies.

Each object of CTO_i, that is planning to activate the next functioning stage and is oriented towards using functions of predicting cases of $\mathcal{K}a_i$ type, has to register in electronic form all the events related to deviations in $Pr_i(CTO_i)$ from the requirements foreseen by technical requirements to CTO_i. This information represents the data regarding the current object state, besides, a series of calculations is implemented by an external system of predicting the possibility of occurring of $\mathcal{K}a_i(CTO_i)$. These data include the following:

- Data regarding CTO_i maintenance and repairs work, performed in the current operation period,
- Data regarding external factors activated by dangers that eventually performed a negative influence on CTO_i, and changes in CTO_i caused by them,
- Data regarding the known features of the functioning process during performing the next stage of the functioning period of CTO_i that is planned to be activated, including data regarding the maintenance staff and some others.

Based on the given data, it becomes possible to solve the whole set of tasks related to implementing the safe functioning of CTO_i. Solving these tasks in the Sr environment is distributed in the following way:

1. Within CTO_i tasks are solved that consist of determining the current value of reliability of single nodes and the system in general, on the basis of which the value of the current system resource is determined.
2. The task of determining the influence of human factor on the CTO_i functioning process is solved.
3. Within the common system tools, external factors are determined that can be activated by dangers typical for the conditions of the current state of CTO_i functioning process.
4. On the basis of data from items 2 and 3, necessary protection measures for CTO_i are determined, that can ensure the given safety level, and strategies are formed for continuing the CTO_i functioning process under the influence of external and internal attacks on CTO_i.
5. On the basis of data obtained as a result of solving tasks given in item 4, it is possible to predict the occurrence of $\mathcal{K}a_i(CTO_i)$ and estimate the prediction accuracy.

4. Determining the accuracy estimation of prediction of $\mathcal{K}a_i(CTO_i)$ occurrence on the basis of risk concepts

One of the possible approaches to estimating the prediction accuracy is based on analysis of capabilities of the prediction model itself. This approach makes sense in the case when a prediction model $M(PG)$ is an analytic function. Within the scope of researched approach, a prediction model is a complex of single models related to each other not only by reciprocal data exchange, but also by the process of protecting CTO_i from $\mathcal{K}a_i$ in general. An example of these components can be danger models $M(Nb_i)$, models of single functioning processes of CTO_i, or $MF[Pr_{ij}(CTO_i)]$, models of diagnosing single nodes $MD_i(V_i(CTO_i))$, models of attacks $M(At_i)$ of various types and other models, using which can become reasonable to increase the prediction accuracy. Estimating the accuracy of predicting dangerous events is necessary because of various cost of losses that can be caused by influence on CTO_i of a dangerous event Vp_i^N, that depends on the prediction accuracy. For example, if the accuracy of determining the moment of occurrence of event Vp_i^N is high enough, and the time interval between the moment of completing the prediction and the moment of occurrence of the predicted event is high enough, there are more possibilities to implement the processes of withstanding the influence of Vp_i^N on $Pr_i(CTO_i)$. Thus, the less accurate a prediction of a certain Vp_i^N event is, the greater are losses the CTO_i object can suffer. So, prediction accuracy can be evaluated by the value of losses that can be caused by a negative influence of Vp_i^N on CTO_i which was not fully withstood. In many cases relating to CTO_i this situation takes place when withstanding the occurring malfunctions is not fully implemented, for instance, when its development process is eliminated but the changes that appeared in CTO_i are blocked and left as some sort of anomaly. Within the scope of this approach, in order to increase prediction accuracy, it is not always necessary to modify the prediction model itself, but it is sufficient to extend the

prediction system with additional components, so that using the results of their functioning can lead to increasing the prediction accuracy.

Adding new components to the prediction system $S(PG_i)$ can be related to increasing expenses on $S(PG_i)$, or to increasing the prediction price.

On the other side, the value of prediction accuracy can be correlated to the value of risk of losses that are measured by their corresponding costs. Thus, we can assume that models of risk estimating can be used to estimate the prediction accuracy [9].

The value of risk of a catastrophic event occurrence is an integral parameter that unites all the factors that influence the state of CTO_i. Each object has a certain price that includes all the aspects determining this price, so we will define the risk value $R(CTO_i)$ as the cost of expenses determined by the value $R(CTO_i)$]10]. The risk values are reasonable to assume as discrete and correlate each value to various situations that occur in Sr regarding CTO_i and occur within the STO_i themselves. These situations will include the following:

1. Violations of a process $Pr_i(CTO_i)$, that can be eliminated and restore the corresponding normal mode of performing $Pr_i(CTO_i)$, as well as emergency situations at CTO_i that are detected by the safety system $SB_i(CTO_i)$, provided there are prepared measures in SB_i to remove them.
2. Unexpected emergency situations that are caused by attacks of the At_i^N type, for withstanding which the components of SB_i are not prepared.
3. Catastrophic situations that are foreseen, which enables the possibility, by changing the functioning strategy, to avoid big losses that characterize the corresponding catastrophes.
4. Unforeseen catastrophic situations, that lead to rather big losses, and other situations.

Each of the given situations can be estimated by a certain loss value. Thus, we will measure the risk value of occurrence of one or other situation by the corresponding values of possible losses.

Violations of $Pr_i(CTO_i)$, caused by internal factors, are discovered by diagnostic systems and are eliminated by the maintenance staff or automatically, if there are corresponding tools for that. If violations are caused by external factors, that are interpreted as attacks and recognized by the SB_i system, then the SB_i system, besides recognition, implements withstanding the corresponding attacks.

Violations of $Pr_i(CTO_i)$ by internal factors that are unexpected, that lead to occurrence of emergency situations, and external attacks activated by dangers for recognizing which the tools of the SB_i system are not prepared, require using the corresponding prediction models. In the first case, these models are a part of SB_i from CTO_i that predict the malfunction development, while in the second case these models are prediction models that describe the occurrence conditions of events of Vp_i^N type and transfer the corresponding data to SB_i for the latter to implement the processes of withstanding the possible violations in $Pr_i(CTO_i)$, especially those that can lead to $\mathcal{K}a_i(CTO_i)$.

In cases when external attacks are unexpected and their analysis confirms the possibility of occurrence of catastrophic situations, that are described with a certain approximation by the corresponding parameters, one of ways to withstand them, implemented by the SB_i system, is to initiate changes in the functioning strategy of the corresponding CTO_i so that CTO_i could evade the catastrophe. This analysis lies in using synthesis of models of predicting external attacks and models of diagnosing the functioning process of CTO_i system.

Tasks that are related to the given situations, except the tasks of determining $\mathcal{K}a_i(CTO_i)$, are solved by tools of the SB_i system from CTO_i. The completeness of solving the tasks of predicting, recognizing and determining the withstanding methods for negative events Vp_i^N, that lead to occurrence of $\mathcal{K}a_i(CTO_i)$, is provided by the fact that these tasks are solved by the tools common for all object of CTO_i type that are placed in Sr.

5. Conclusions

In the paper, different approaches have been analyzed for implementing the prediction process which allows to choose the most corresponding method of predicting random events that can lead to occurrence of a catastrophic situation. Different attack types are reviewed, each of which defines the features of implementing protection of a technical object from the corresponding attacks. This allows to implement the necessary measures of protecting the technical object.

An organization of system of predicting random events, that negatively influence or act on the corresponding technical object, is researched. Attacks are reviewed as well as situations that can lead to occurrence of catastrophic situations on an object. For that, the components of a prediction system are defined that interact with each other during the implementation of a prediction.

Analysis of data necessary to use within the prediction is performed. Proofs are given that in most cases catastrophic events are caused by super-rare random events, occurrence of which can be interpreted as influence of the corresponding attacks on an object. The paper contains analysis and proof that the accuracy of a prediction implemented by the corresponding system can be estimated by a risk value, that defined the value of losses that can be caused by insufficient prediction accuracy. In this case, managing the prediction accuracy can be performed by increasing or decreasing the number of components that form the system of predicting super-rare random events.

6. References

[1] Yakovets Y.V.: Theoretic basics and models of long-term macroeconomic prediction, Moscow, MIPS-NK, Tekhnologiya TD, 2004, 237 p.

[2] Korostil J.: Features of protection of technical objects against negative exposure. Measurement, Automation, Monitoring. Jul. 2016, no. 07, vol. 62.

[3] Wesołowski Z.: Analiza niezawodnościowa niestacjonarnych systemów czasu rzeczywistego. Warszawa WAT, 2006, 198 p.

[4] Devyanin P.N., Saderdinov A.A., Trainev V.A. and others: Informational safety of an enterprise. Moscow, 2006, p. 335.

[5] Polovko A.M., Gurov S.V.: Basics of reliability theory. BHV. Petersburg, 2006, p. 704.

[6] Korbicz J., Koscielny M., Kowalczyk Z., Cholewa W. (eds.): Diagnostyka procesów. Modele. Metody sztucznej inteligencji. Zastosowania. Warszawa: WNT, 2002, 828 p.

[7] Lukatski A: Wykrywanie włamań i aktywna ochrona danych. Gliwice: Helion, 2005, 511 p.

[8] Messier R.: Penetration Testing Basics. Apress, 2016, 140 p.

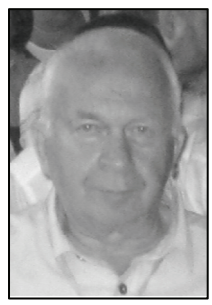
[9] Benin V.E., Korolev V.Yu., Liu Lixin: Asymptote behavior of generalized risk processes. Acta Mathematica Sinica Sinica, English Series, 2004, V. 20, No 2, pp. 340-356.

[10] Beard R.E., Pentikainen T., Pesonen E.:Risk Theory. London: Chapman and Hall, 1978, 475 p.

Received: 06.05.2017 Paper reviewed Accepted: 02.07.2017

Prof. Yuriy KOROSTIL, DSc

He works at the Faculty of Navigation in the Maritime University of Szczecin since 2011. Research interests: security of information digital systems, the safety of complex technical objects, taking into account social factors, technical objects protection systems



e-mail: j.korostil@am.szczecin.pl