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

Features of protection of technical objects against negative exposure

Abstract

This paper presents research of different classes of attacks against complex technical objects. Attacks are differentiated into different classes on the basis of analysis of attack features which reflect the possible methods of attack interaction with the security system. The developed methods of formal description of attacks and defense methods on the level of their logical approximation allow describing tasks of withstanding attacks for defense tools with enough certainty. Thanks to the proposed interpretation of attack interaction with a defense object and defense tools, it has become possible to determine approaches to the extension of the defense system by adding new tools oriented towards withstanding new attacks.

Keywords: attack, prognosis, security system, model, technical object, tools.

1. Introduction

A complex technical object (CTO) generally falls under negative influence of series of factors, of both internal and external nature. The source of these factors is a threat factor Nb_i. The danger Nb_i at random time moments t_i activates negative influences on CTO which will be called attacks At_i with respect to the established terminology in the information security sphere [1]. An attack At_i can be a certain sequence of events $At_i = \{Vp_{i1} * ... * Vp_{im}\}$ or a single event Vp_i, both of which are random. Randomness of such an event is determined not only by the moment of its occurrence t_i but also by series of other parameters, for example, describing a character of the influence on CTO or a force of such an influence, for instance, weather conditions. The technical object CTO as a rule, contains a security system SB which has the main task of protecting CTO from the negative influence of random events Vp_i. It is natural to assume that such a system contains a series of subsystems Sb_i and each of them is oriented towards the specific task class or the different Nb_i types. The SB system solves the tasks of detecting negative Vp_i recognizing the attack type At_i and, corresponding to At_i provides counter-measurements against the corresponding attack. The above-listed functions can be displayed as the following relation scheme:

$$Nb_i \to At_i \to Vp_i \to SB_i[RA_i \to PAr_i] \to (\delta At_i \lor \neg At_i) \to CTO \qquad (1)$$

where RA_i is the recognition of Vp_i, PAr_i is the system of withstanding At_i, δAt_i is a residual effect of attack on the CTO object.

SB_i system has to react to an occurrence of Vp_i in real time mode, which is determined by speed of occurrence and influence of events Vp_i that form the attack on CTO. If the real time mode is interpreted as time intervals of existence of factors that determine the process of affecting CTO it is necessary to introduce the following time intervals: ΔT_i is a time interval during which the attack At_i is affecting CTO. During a certain time interval Δt_i the system SB_i has to recognize Vp_i and activate the corresponding counter-measure PAr_i. It is natural to assume that information regarding At_i and the actual At_i attack itself can be separated in space. In this case, time relations between the interval of At_i influence on the CTO and the interval of SB_i reaction to At_i have to meet the following relation:

$$[(\Delta T_i < \Delta t_i)\&\big(At_i(\Delta T_i) \to SB_i(\Delta t_i)\big)] \to \neg(At_i \to CTO). \qquad (2)$$

In a usual situation, which corresponds with functioning of CTO, there can be a condition when information regarding Vp_i and the Vp_i itself are inseparable in space. A possible example of this is an attack on the information maintenance system or the CTO functioning process control system [2]. The two above-mentioned cases are different because separating the information regarding Vp_i and the Vp_i itself generally causes an increase in ΔT_i interval for Vp_i. Nevertheless, the Δt_i interval remains the same because it is determined by the possibilities of the SB_i system.

A security system can be distributed among all the objects that are related to maintaining security of SB_i. Because other occurrences, besides negative ones, can exist and cause no harm to the CTO, tools for preliminary data analysis are necessary to use in the SB_i. These tools are called PAD or the tools of preliminary analysis of data. A PAD system can be composed independently for each type of Nb_i, which simplifies the task of input data analysis to determine whether they are acceptable or belong to prerequisites for the occurrence of negative events. These tools can be some approximations of a model of fragments Nb_i which lead to Vp_i. In the simplest case, it could be models of threshold analyzers of the values of input parameters. Let us introduce some definitions regarding the influence of At_i on CTO.

Definition 1. If an influence of At_i on CTO causes the CTO functioning process to stop or to change, leading to failure of CTO to comply with its determined goals, then CTO starts to have malfunctions, and At_i goes to a class of successful At_i^U

$$[(At_i \to CTO)\&\big(CTO \to A(CTO)\big)] \to (At_i \to At_i^U). \qquad (3)$$

Here, $A(CTO)$ is a malfunctioning condition of CTO.

Definition 2. If an influence of At_i on CTO moved it to $A(CTO)$ and $A(CTO)$ started causing harm to the environment SOk_i, then CTO goes to the emergency state $N(CTO)$.

$$[(At_i \to CTO)\&(CTO \to N(CTO)\&(N(CTO) \to SOk_i)] \to [CTO \to A(CTO)]\&(At_i \to At_i^N)], \qquad (4)$$

where At_i^N is an unexpected attack. The mentioned definitions require the following remarks. There are types of CTO which include the environment components into themselves for a certain time interval. Thus, if a negative influence appears on these components as a result of transition $CTO \to N(CTO)$, this $N(CTO)$ does not go to the condition $A(CTO)$, which is formally described by the following relation:

$$\{[At_i \to [CTO\&E(SOk_i)]\&[CTO \to N(CTO)]\& [N(CTO) \to E(SOk_i)]\} \to [N(CTO) \to A(CTO)]. \qquad (4)$$

Here, $E(SOk_i)$ are the environment components.

2. The basics

Having introduced the definition of an emergency situation on CTO or an accident on CTO, it is necessary to consider a task of detecting the corresponding prerequisites of the accidents. A common reason for an accident to occur is an existing attack. Because not every attack can lead to an accident, it is necessary to introduce their certain classification which is based on the analysis of interconnection between the attacks and defense tools. The formal description of attacks and defense tools will be made through means of mathematical logics [3]. Keeping this in mind, let us consider the following statement.

Statement 1. Any attack At_i has a logical structure $\mathfrak{H}(At_i)$ which is described by the following logical formula or the formula system:

$$\mathfrak{H}(At_i) = \mathcal{L}(L_{i1}, \ldots, L_{im}), \tag{5}$$

where $\mathfrak{H}(At_i)$ is the logical structure of an attack At_i, $\mathcal{L}$ is a logical function that describes interconnection between certain logical formulas.

This statement can be proven in the following way: any attack At_i regardless of its physical nature consists of a series of some events $\{Vp_{i1}, \ldots, Vp_{im}\}$. Each Vp_{ij} can occur or not occur, which is allowed by interpretation of Vp_{ij} on the set $\{0,1\}$. The process which determines an occurrence of a single event Vp_{ij} is described by a set of parameters $\{x_{i1}, \ldots, x_{im}\}$. Each parameter x_{ij}, if it describes a process of occurrence of Vp_{ij}, has a subset of values which allow it to determine the possibility of occurrence of Vp_{ij} or the impossibility of occurrence of Vp_{ij}. This allows an interpretation of parameter values on a binary set. Let us assume that within the scope of the model $M(Vp_i)$ that describes the process of occurrence of Vp_{ij} there are several parameters $\{x_{i1}, \ldots, x_{im}\}$. Because the result of interaction of these parameters is either occurrence or non-occurrence of Vp_{ij} functional interconnections allow the possibility to interpret results of their implementation on the binary set $\{0,1\}$. If the parameters $\{x_{i1}, \ldots, x_{im}\}$ and the results of their interaction within the scope of functions $\{f_{i1}, \ldots, f_{im}\}$ that describe the model $M(Vp_i)$ allow the binary interpretation, the corresponding model $M(Vp_i)$ allows an approximation of its description by the description of logical formulas. This means that $M(Vp_i) \Rightarrow \mathcal{L}(L_{i1}, \ldots, L_{im})$. Because $At_i = F(Vp_{i1}, \ldots, Vp_{im})$ and At_i allows the binary interpretation, Vp_{ij} allows the binary interpretation, so the function F which describes interrelation between At_i and $\{Vp_{i1}, \ldots, Vp_{im}\}$ allows the logical approximation of description of the process implemented by the function F. This proves the above-mentioned statement.

Based on the mentioned statement, we can state that the description of an attack At_i can be approximated as logical systems. Using this method of describing At_i allows shortening the description of At_i while preserving the description of logic of their functioning in a certain object domain. The second advantage of using $\mathfrak{H}(At_i)$ is the fact that such a description allows in many cases to evade the necessity of using functional dependencies between the parameters $Vp_i = f(x_{i1}, \ldots, x_{im})$, which can turn out to be unknown for various reasons.

Different methods of attack classification are possible. These methods most often depend on methods of detecting and withstanding attacks [4,5]. Let us examine the classification of attack types which is based on the analysis of interaction of At_i with the security system SB_i. Let us assume that SB_i consists of the following components:

- the component of samples $E(At_i)$ of attacks known to the SB_i,
- the component of tools of withstanding the attacks $ZG = \{Zg_1, \ldots, Zg_k\}$,
- the component of controlling the tools of SB_i, or USB_i,
- the component of predicting random events VP_i.

Definition 3. If an attack At_i is not identified by SB_i by using $E(At_i)$, but its logical structure $\mathcal{L}(At_i)$ can be deduced from $\mathfrak{H}[E(At_i)]$ and the data obtained as a result of implementation of predicting the current attack, then this At_i is an attack which differs from attacks in $E(At_i)$ by having unknown fragments $\mathcal{L}_i^* \in \mathfrak{H}_i(At_i)$, and the corresponding attack is successful, or $At_i \rightarrow At_i^U$.

Formally, this definition can be written as the following relation:

$$\{\mathcal{L}_i(At_i) >\notin [E[\mathcal{L}_i(At_j)]]\} \& \left\{\{E[\mathcal{L}_i(At_j)]\&R(At_i)\right\} \rightarrow \\ \mathcal{L}_i(At_i)\} \rightarrow \left(At_i \rightarrow At_i^U\right), \tag{6}$$

where At_i^U is a successful attack, $R(At_i)$ is a description of a logical scheme of the attack At_i based on the data obtained as a result of predicting At_i.

Successful attacks will be classified as attacks with modified parameter values or modified fragments of logical formulas in their descriptions, which can be written as: $At_i^U = \varphi(At_i)$, where φ is a function of modifying At_i, that is used in the subject area making up a set of dangers $NB = \{Nb_1, \ldots, Nb_k\}$.

Definition 4. If an attack is not identified by SB_i based on using $E(At_i)$ and is not deducible from $\mathfrak{H}_i[E(At_i)]$ and the data obtained as a result of predicting the current attack, this attack At_i belongs to the attacks of the class At_i^N, which belong to unexpected attacks.

Attack description is approximated by logical formulas with the purpose of conducting an attack analysis. Thus, it is reasonable to use logical formulas to approximate the description of functional possibilities of the defense tools Zg_i, that will be written as $\mathcal{L}_i(Zg_i)$. Because Zg_i are oriented towards withstanding At_i , the logical interpretation of the process of uniting the systems $\{\mathcal{L}_i(At_i)\&\mathcal{L}_i(Zg_i)\}$ is that the corresponding system of logical formulas went from one state, for example, $\mathcal{L}_i(At_i) = 1$, to the state $\mathcal{L}_i(At_i) = 0$ as a result of interaction of $\mathcal{L}_i(At_i)$ with $\mathcal{L}_i(Zg_i)$, which can be described by the following relation:

$$\{\mathcal{L}_i(At_i)\&\mathcal{L}_i(Zg_i)\&[\mathcal{L}_i(At_i) = 1]\} \rightarrow [\mathcal{L}_i^*(At_i) = 0]. \tag{7}$$

The accepted values of the logical formula $\mathcal{L}_i(At_i)$ are determined by the result of At_i functioning. If it is successful, then $At_i \rightarrow At_i^U$ and $\mathcal{L}_i(At_i) = 1$, and vice-versa.

3. The task of attack identification

Attack identification in this paper is implemented on the basis of its description using the logical formulas. In accordance with the statement (1), the formula that describes an attack uses attack parameters of the same name as logical variables x_i. If a certain parameter takes the values from its range of definition which provide the successful attack functioning on a single fragment of all At_i functioning process, or $\varphi_i[Pr_i(At_i)]$, then this variable value is assumed to be «1» and vice-versa. Interpretation of functions $\varphi_i = f(x_j, \ldots, x_k)$ which make up $Pr_i(At_i)$ is formed similarly. Thus, we can assume that $\mathfrak{H}(At_i) = 1$. The correctness of such an assumption fully arises from the statement (1). So let us consider the following definitions.

Definition 5. If $\mathfrak{H}\,(At_i) = 1$, the corresponding At_i is built correctly in respect of the goal of its usage.

It is natural to assume that $\mathfrak{H}\,(Zg_i)$ has to influence the $\mathfrak{H}\,(At_i)$ in such a way that, as a result of this influence, the synthesized logical system $\mathfrak{H}_i^*\,(At_i, Zg_i) = F\{\mathfrak{H}\,(At_i), \mathfrak{H}\,(Zg_i)\}$ led to the relation $\mathfrak{H}_i^*\,(At_i, Zg_i) = 0$. We will show that this interpretation of the influence Zg_i on At_i is fair on the level of their logical description.

Definition 6. The value of the logical formula $\mathfrak{H}\,(Zg_i) = 1$ in the process of synthesis is correlated to the value of the logical formula of the attack $\mathfrak{H}\,(At_i)$=1, which belongs to the class of attacks oriented towards the corresponding defense tool.

This definition represents the functional orientation of defense tools Zg_i to a certain At_i attack class.

Statement 2. If $\mathfrak{H}(At_i)$=1 and $\mathfrak{H}(Zg_i) = 1$, then synthesis of $\mathfrak{H}(At_i)$ and $\mathfrak{H}(Zg_i)$ leads to $\mathfrak{H}_i^*\,(At_i) = 0$, where $\mathfrak{H}_i^*\,(At_i) = F\{\mathfrak{H}\,(At_i), \mathfrak{H}\,(Zg_i)\}$.

The functioning process of the fragment $Pr_i(At_i)$ is as follows. Let $\varphi_i[Pr_i(At_i)]$ be described by the function $y_i = f_i(x_i, x_j)$. Let us assume that $y_i \in Q^+(y_i)$ is a range of values of y_i where its logical interpretation $L(y_i) = 1$. It means that such $x_i \in Q(x_i)$ and $x_j \in Q(x_j)$ are selected that the logical interpretation $f_i(x_i, x_j)$ or $L[f_i(x_i, x_j)] = 1$. Withstanding Zg_i the attack At_i consists of such a change $Q(x_i)$ or $Q(x_j)$ that $L[f_i(x_i, x_j)] = 0$. To do this, it is enough to change the range of definitions $Q^{+}(x_i) \rightarrow Q^{-}(x_i)$. This description of influence of Zg_i on At_i is correct because Zg_i is a component of SB_i and CTO in general. It means that Zg_i is implemented in such a way that it could change the parameter values in the range of definitions $Q(x_i)$, defined in the subject area of CTO interpretation. In the scope of a synthesis process, on the basis of using Zg_i the $x_i \in L(x_i, x_j)$ is replaced with x_i^1, for which the following is true: $[x_i \in Q_i^{+}(x_i)] \rightarrow [x_i^1 \in Q_i^{-}(x_i^1)]$. It means that the range of definitions of x_i is changed (e.g., if x_i is an address in a computer network, and Zg_i is a firewall, changing the range of definitions for x_i requires to transfer the address which the current value of x_i corresponds to into the list of addresses forbidden for accessing the protected local network). If this influence of Zg_i on At_i did not lead to $\mathfrak{H}_i^{*}(At_i) = 0$, then Zg_i goes to the next fragment $\varphi_{i+1}[Pr_i(At_i)]$ and performs the same replacement for $f_{i+1}(x_i, x_j)$. This process is repeated until x_{i+k}^{m} turns out to be the last one in $\mathfrak{H}(At_i)$. If it also turns out that $\mathfrak{H}_i^{*}(At_i) = 0$, then withstanding Zg_i the attack At_i ended successfully.

The mentioned statement uses approximation of descriptions of Zg_i and At_i by logical formulas, and ranges of definitions of parameters x_i are formed in the subject area of the interpretation W_i of the attack object. The statement (2) is the basis for implementing the identification of At_i, which is necessary to choose the corresponding defense tool Zg_i.

4. Features of using prediction in the tasks of protection of technical objects

The process of identifying At_i requires a certain time for SB to execute the corresponding functions. Because the speed of implementing the processes of At_i is determined by the development speed of At_i in the environment W_i, where At_i is transferred and activated, it can turn out that the speed of identification and withstanding is not high enough. As it was stated before, we will interpret the speed of process functioning by time intervals necessary to implement the corresponding processes. The necessary correlation between the given time intervals is given in the statement (2). In order to ensure the relation $\Delta T_i < \Delta t_i$, the following approaches can be used:

- to solve the defense task on the basis of using the consequent partial withstanding the activated attack At_i,
- to increase the value Δt_i by solving the tasks of predicting random events which identify the attack At_i,
- to solve the task of implementing the interaction with dangers Nb_i, regardless of whether a certain Nb_i has activated the attack At_i on the CTO object or not.

In this case, let us examine certain aspects of the approach based on using the prediction processes [6]. Within the scope of a prediction system (SPR) it is possible to solve not only the tasks of determining the time interval δt_i, after which the predictable event VP_i can occur, but also the tasks of determining the possible values of the parameters characterizing the predictable events and the attack At_i in general. In this case we can write that $\Delta t_i^P = \Delta t_i + \delta t_i$. Because δt_i is a parameter of SPR, we can assume that, within certain limits, its value can be chosen so that it would be necessary for solving the defense tasks. It is obvious that prediction of parameters x_i that characterize VP_i is synchronized with predicting δt_i. It is obvious that each predictable value has its own prediction function in the SPR [7].

Identification of an attack class, which can distinguish attacks of classes At_i, At_i^U, At_i^N, is partially implemented in the system of preliminary analysis of input data PAD and in the system of attack recognition RA, which works with data obtained as a result of prediction. Solving the task of defining which attack class a certain At_i corresponds to is necessary to solve the task of SB_i withstanding the corresponding attack. Because there is too little given data about the attacks At_i, especially At_i^U, At_i^N, it is necessary to review the possible interrelations between the different attack classes. Let us assume, as input data regarding the attack type At_i, that the attacks of the At_i class consist of a certain sequence of rare enough events in time, which is characterized by a certain known intensity λ. It is natural to assume that the events of the At_i class obey the Poisson distribution [8,9]: $P_m = a^m e^{-\lambda}/m!$, where m is a number of independent events during the same time intervals.

Let us consider the differences between At_i and At_i^U. As goes from the definitions (3) and (4), At_i has $\mathfrak{H}(At_i) \in \mathfrak{H}[E(At_i)]$. An attack of the class At_i^U has an assortment of parameters that correspond to $E(At_i)$. The difference of At_i^U and At_i lies in the fact that At_i^U contains the functional fragment $\varphi_i^U[\mathcal{L}_i(At_i^U)]$ that does not coincide with $\varphi_i[\mathcal{L}_i(At_i\ )]\in \mathcal{L}_i(At_i)$. It means that the method of using known parameters $x_i \in \mathfrak{H}(At_i)$ is different from methods of using the same parameters $x_i \in \mathfrak{H}(At_i^U)$ and these methods differ in descriptions determined by the functions φ_i^U and φ_i. Let us assume that At_i^U occur much less often. It means that each current attack At_i^U is structurally new regarding the previous attacks At_{i-1}^U. Forming new At_{i+1}^U regarding At_i^U requires much more expenses from Nb_i comparing to using At_{i+1}, which differs from At_i in values of attack parameters, while keeping its structure or logical scheme. Regarding the attacks of the class At_i^N let us define the following hypothesis.

Hypothesis 1. The occurrence probability of an attack of the class At_i^N increases when the occurrence frequency of attacks of the class At_i^U increases.

Because the occurrence frequency of an attack allows to interpret the occurrence probability of At_i^U, the following relation can be written:

$$P(At_i^N) = f[P(At_i^U)]. \tag{8}$$

When an attack At_i^N occurs, as in the case of other attacks, a task appears of withstanding this attack with the system SB. Because the attack belongs to the class of unexpected or unknown attacks, there are no corresponding defense tools $Zg_i\ (At_i^N)$ in the SB. Because of this, the task of protecting the CTO from the At_i^N can be solved on the basis of the following approaches: partial withstanding the attack; forming the $Zg_i(At_i^N)$, that is oriented towards the At_i^N with the following usage of the corresponding defense tool.

Let us consider the possibility of implementing the second approach. The attack At_i^N, as well as attacks At_i и At_i^U, has an approximate logical description $\mathcal{L}_i(At_i^N)$. Because the attack class At_i^U is described by the same parameters that the attack class At_i and is different from the latter by using new logical fragments $\varphi_i^{*}(At_i^U)$, it is necessary to determine the differences of At_i^N regarding At_i^U. Such a difference lies in using new parameters $\{x_i^N, \dots, x_{i+k}^N\}$, absent in the At_i and At_i^U, that use the new parameters x_i^N along with parameters $x_i^U \in At_i^U$ and $x_i \in At_i$. The parameters x_i^N, which were not used in Zg_i, have to be present in the subject area $W_i(CTO)$. If this condition is not true, the attack At_i^N is not correct because it cannot affect the CTO.

Based on the statement (2), we can assume that Zg_i, during the synthesis with the corresponding system $\mathfrak{H}(At_i)$, leads to changing the value of logical formulas which make up the system: $\mathfrak{H}^S[\mathfrak{H}(At_i), \mathfrak{H}(Zg_i)]$. It means that the logical descriptions $\mathfrak{H}(At_i)$ and $\mathfrak{H}(Zg_i)$ are two logical antagonisms. Let us introduce the following definition.

Definition 6. Two logical formulas $L_i(x_{i1},\dots, x_{im}\}$ and $L_j(x_{j1},\dots, x_{jk}\}$ are antagonistic, or mutual antagonisms, if $L_i(x_{i1},\dots, x_{im}\}$=1 and $L_j(x_{j1},\dots, x_{jk}\} = 1$, and the result of their synthesis is:

$$Sin\{L_i(x_{i1}, \dots, x_{im}\}, L_j(x_{j1}, \dots, x_{jk}\}\} = \mathfrak{H}^S(L_i, L_j) = 0. \tag{9}$$

In order to successfully build $\mathfrak{H}[L_i(At_i^N)]$, the following has to be performed:

1. To expand the system $\mathfrak{H}(Zg_1, \dots, Zg_k)$ by new descriptions that use the new formulas $\mathcal{L}_i(x_{i1}^N, \dots, x_{im}^N)$.
2. To expand $E(At_i)$ by new descriptions that correspond with $\mathfrak{H}[L_i(At_i^N)]$.

Statement 3. For a random At_i^N a $\mathfrak{H}[L_i(At_i^N)]$ can be built using the structural descriptions $\mathcal{L}_i(CTO)$ and parameters $\{x_{i1}^N, \dots, x_{im}^N\}$, obtained from the prediction system.

Proof. Any CTO has the description $\mathfrak{H}(CTO)$, which is a logical approximation of the full description of CTO. Logical functions ℓ_i represent links between certain CTO elements and the logic of their functioning. Any attack is oriented to disrupt this link or the functioning process. It means that the parameters $x_i^a \in At_i$ are defined in the range of values of the parameters $x_i^S \in CTO$. Interaction $\{x_{i1}^a, \dots, x_{im}^a\}$ within the limits of $\mathcal{L}_i^a(x_{i1}^a, \dots, x_{im}^a)$ is described by the processes, oriented towards withstanding the processes $\mathcal{L}_i^S(x_{i1}^S, \dots, x_{im}^S)$. The interaction between At_i and CTO on the logical level is modeled by the synthesis process $\mathcal{L}_i^a(L_{i1}^a, \dots, L_{im}^a)$ with $\mathcal{L}_i^S(L_{i1}^S, \dots, L_{im}^S)$, as the result of which the following relation is obtained: $\mathrm{Sin}[\mathcal{L}_i^a, \mathcal{L}_i^S] = 0$. It means that during the influence of an attack on the CTO the latter can be identified as an attack of the class At_i^N if $\{x_{i1}^a, \dots, x_{im}^a\} \in At_i^N$ are identified on the basis of data about $\{x_{i1}^S, \dots, x_{im}^S\}$, that correspond to the CTO and are not present in $\mathfrak{H}\{E[(At_i)\&(At_i^U)]\}$. To build $\mathcal{L}_i^N(x_{i1}^N, \dots, x_{im}^N) \subset At_i^U$, known $\mathcal{L}_i^S(L_{i1}^S, \dots, L_{im}^S)$ are used. To implement the processes of synthesis of $\mathcal{L}_i^S(L_{i1}^S, \dots, L_{im}^S)$ and $\mathcal{L}_i^a = \mathcal{L}_i^a(At_i^N)$, output procedures are used, where the current elements are chosen on the basis of antagonism conditions. On the basis of implementation of the mentioned procedures the output $\mathfrak{H}[\mathcal{L}_i(CTO) \rightarrow \mathfrak{H}[\mathcal{L}_i^N(At_i^N)]$ is implemented, which proves the statement.

Building $\mathcal{L}_i^N(At_i^N)$ requires obtaining the parameters $x_{ij}^a \in At_i^N$, and it is also necessary to have enough time Δt_i to build $\mathcal{L}_i^N(At_i^N)$. To provide the necessary amount of time Δt_i, prediction of the corresponding events $\{Vp_{i1}, \dots, Vp_{im}\} \subset At_i^N$ is used. Prediction is performed on the basis of the relation (8). To do this, let us replace the implicit function f from this relation with a function that describes the Cox processes [10]. These processes are twice stochastic Poisson processes, and their interpretation is useful to describe two stochastic processes from the relation (8). The first stochastic process is the process of At_i^U occurrence, which controls the second stochastic process of At_i^N occurrence. In this case the model of predicting At_i^N is based on using the following relation:

$$P(N^*(t) = k) = e^{-\lambda(t)}[(\Lambda(t))^k / k!],$$

where $\Lambda(t)$ is a positive function which describes the intensity of occurrence of events, $N^*(t)$ is a non-uniform Poisson flow of At_i^N.

5. Summary

This paper contains the analysis of tasks related to the safety of CTO. This task is reviewed in the context of analysis of attacks which are divided into three classes. On the basis of such division, possible methods of detecting attacks of different classes as well as the possibilities of withstanding these attacks are investigated.

There is examined a system of predicting random events as one of the important security system components that allow identifying attacks.

Research of methods of detecting, analyzing and withstanding attacks on the basis of using their description on the level of the logical approximation of such description allows one to correctly build defense processes for the attack object on a quite general level. This enables linking the processes of withstanding attacks with the parameters of the defense object. The correctness of this approach to analyzing the tasks for defense tools to withstand attacks that influence the object is based on the proofs, given in the paper, of the corresponding statements.

The problem of providing safety of technical objects is reviewed in the scope of all components which are in some way connected with the safety of technical objects. This allows considering the possibility to research safety of technical objects not only within the limit of the local security systems, but also taking into account the tools which can be included into the security system regardless of whether these tools are localized in the scope of the defense object or not.

6. References

[1] Stalling W.: Network and Internet-work Security. Principles and Practice, Prentice Hall. Inc. - 451 p. 1994.

[2] Lusznikow E.M.: Ship's navigational safety. Szczecin. Maritime University, 201 p. 2001.

[3] Curry H.: Foundations of Mathematical Logic. Moscow: Mir, 567 p. 1969.

[4] Lukatski A.: Wykrywanie włamań i aktywna ochrona danych. Poland, Hellion, 511 p. 2005.

[5] Liderman K.: Bezpieczeństwo informacyjne. Warszawa, PWN, 218 p., 2012.

[6] Shurigin A.M.: Applied Stochastics: Robustness, Estimation, Prognosis. Moscow, Finances and Statistics. 224 p., 2005.

[7] Bidyuk P.I., Romanenko V.D., Timoshchuk O.L.: Analysis of Time Series. Kyiv, NTUU "KPI", 600 p., 2013.

[8] Ventzel E.S.: Probability Theory. Moscow, Nauka, 545 p., 1969.

[9] Gajek L., Kaluszka M.: Wnioskowanie statystyczne. Modele i Metody. Warszawa, WNT, 304 p., 2000.

[10] Korolev V.Yu.: A general theorem on the limit behavior of superposition's of independent random processes with applications to Cox processes. J. Math. Sciences. Vol. 81, no 5, pp. 2950 – 2956, 1996.

Received: 18.02.2016 *Paper reviewed* *Accepted: 01.06.2016*

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