УДК 004.02+004.05+005.93+ 510.3 https://doi.org/10.15407/pp2021.02.016

Y.S. Rodin, I.P.Sinitsyn

SECURITY BASIC MODEL FOR APPLIED TASKS OF THE DISTRIBUTED INFORMATION SYSTEM

The tasks of modelling and the components of the basic model of applied task protection of a distributed information system have been considered. The measurement and relationship of security parameters, protection, new and reference attacks, anomalies, and threat environments have been proposed. The conditions of threats, attacks and, consequently, inconsistencies in the results of applied tasks are proved. At the beginning of the article the concept of a distributed information system, system of applied tasks, modern trends of zero-trust architecture in building information security systems are discussed. Further, it gives an overview of existing methods of detection and counteraction to attacks based on reference knowledge bases. To improve the level of security it is proposed to analyze the causes of attacks, namely hazards and threats to the system.

Attacks, hazards and threats are considered as structured processes that affect the internal and external environment of the system of the applied tasks with a further impact on the output of these tasks. The concepts of security level and security level of a distributed information system are introduced, as well as the concepts of applied task, environment, and user contradictions. As the logical metrics of discrepancy detection the apparatus of semantic analysis is proposed, which based on the reference knowledge base, the apparatus of text transformations should be applied at the stage of loading of applied task and describe the input and output data, requirements to the environment of the task solution.

The result of the research is the proposed method for identifying additional data about hazards, threats, attacks, countermeasures to attacks, applied task-solving. This data is generated from the reference and augmented textual descriptions derived from the proposed contradictions. By building additional reference images of threats, attacks, countermeasures, it becomes possible to prevent the activation of new attacks on the distributed information system.

Keywords: information, security, anomaly, attack, model, applied task, distributed system, semantics.

Introduction

A distributed information system (RIS) is now the backbone of the infrastructure of any organization dealing with electronic information resources. A RIS is a continuously operating mechanism of interconnected distributed general and application software and hardware, interconnected by telecommunication means. As a single RIS user the organization is interested in maintaining its own applied task. To solve the applied task a RIS consolidates certain resources, which together would be called an application system for solving the user's PSZ problem. It is objective and economically reasonable that the user is only interested in protecting his applied task and the PSZ allocated to this task. Creation of demilitarized zones, physical perimeters of protection of the organization's infrastructure environment, corporate systems for recognition of unauthorized intrusion during remote work of organization's employees does not make sense. The article formalizes the PSZ parameters required to build a basic model of information security of a distributed system.

Problem statement

The rapid dynamics of new cyber threats poses new challenges to managers and developers of information security protections. An important one is the effective identification of new, previously unrecorded threats and attacks, as well as the adaptation of protocol protections for new attacks.

In this paper we consider the task of determining the possibility of danger and threat in relation to the application system solving the user's task. It identifies and analyzes the causes of hazards (Nb_i) and threats (Zg_i), analyzes the relationship between Nb_i, Zg_i and attacks (At_i), affecting the occurrence of anomalies in the *PSZ*. A formalization of an adaptive modeling approach to information security system design is proposed.

Analysis of recent studies and publications

With the migration of enterprise software to cloud locations and many infrastructure services to off-the-shelf cloud services and products (SaaS, IaaS, PaaS) in many organizations, a new architecture for building information security is emerging - the adaptive security approach. The main principles of adaptive architecture are proactive continuous threat monitoring, risk auditing, and a shift from single tunneling access of valuable resources to contextual access [1]. The contextual approach to providing access to resources involves defining the requirements for the applied task that orders the resources, continuously monitoring and adapting these requirements.

Each PZa_i for which information resources are commissioned, which the *PSZ* will use to implement its operational processes, must consolidate relevant resources, which also include a description of the data and *RIS* requirements. These are:

- the input information that characterizes the *PSZ* system and is used for its functioning,

- general requirements for the functionality of the resources and their parameters characterizing the *RIS* system,

- the required overall security levels and security values of the individual designated processes, which can be implemented within one or some individual PZa_i of the *PSZ* system,

- the requirements for ensuring the required safety value of the operation of the individual tasks of the PZa_i ∋ *PSZ*,

- the required measure of recoverability of the individual PZa_i in the case of successful completion of an attack on PZa_i by an appropriate attack.

An important function of *PSZ* defense processes is the recognition and identification of attacks At_i and recognition of anomalies An_i, which activate attacks in *PSZ* [2]. Anomaly recognition An_i and attack recognition At_i are quite different from each other. Attack recognition At_i is implemented based on the use of descriptions of the reference images of attacks $E(At_i)$, which are in the database of the system *RSB*. Recognition of anomalies An_i is implemented based on the analysis of deviations of the parameters of the environment in which they occur, from their threshold values, or $\Delta_j^d(P_i)$. One of the features, which is associated with the difference between $E(At_i)$ and $\Delta_j^d(P_i)$, is that in $E(At_i)$ besides the list of parameters P_i, which can characterize An_i, there are some factors that describe in a certain approximation of the relationship between the parameters $P_i(An_i)$ and parameters $P_i(At_i)$. The second feature, which characterizes the possibility of a relationship between $E(At_i)$ and $\Delta_j^d(P_i)$, is that in $E(At_i)$ the number of parameters P_i should be not less than the number that is necessary to identify the corresponding attack. Since $E(At_i)$ represents some structure, $E(At_i)$ can be represented in the form $\{L = [E_i(At_i)]\} \rightarrow L(E_i)$, for which the relation $E(At_i) = L_i(P_1, \ldots, P_k)$ holds, where L_i is the logical function P_i of the parameters characterizing At_i. The relation between An_i and At_i at the logical level can be described by the relation

$$\{[An_i, E(At_i)] \Rightarrow \neg At_i\} \vee \{[An_i, E(At_i)] \Rightarrow [[An_i \Rightarrow L(At_i)] \rightarrow (An_i \Rightarrow At_i)]\}.$$

If at the final stage $[An_i, E(At_i)] \Rightarrow At_i$, then in *RSB* for At_i there exists an algorithm for counteracting At_i, which we will denote by Ap_i. Such algorithms may differ from each other in characteristics that determine their capabilities and type:

- Algorithm Ap_i that completely neutralizes the impact of the counterattack of At_i by neutralizing all the functions implemented by the attack of At_i,

- Algorithm Ap_i, which neutralizes the capabilities of Zg_i to activate the retaliatory attack, or $Ap_i(At_i) \rightarrow \neg Fk_i(At_i)$, where Fk_i is the activation function of At_i,

- Algorithm Ap_i, which partially counteracts the negative impact of At_i on the object of the attack.

The first type Ap_i implements counter attacks that are in the active state. For example, At_i, which has several interrelated stages of its implementation, encounters counteraction in the second, third or other stages of the implementation process, regardless of whether the attack at each stage realizes its impact on the object, which can result in unacceptable changes in functional parameters. Attack localization in this case

is determined by the presence or absence of impermissible modification in the *PSZ* environment. The second type of counteraction Ap_i is to eliminate the vulnerability points of the system, which were used Zg_i to introduce and activate the attack. The third type of algorithm Ap_i, which counteracts At_i, which is activated, is that the counteraction to the attack is implemented only when the effect of the attack on the corresponding object is manifested in unacceptable changes in the functional parameters of the object of attack. This type of attack counteraction can result in blocking some functions in the attacked object, which is *PSZ*.

In addition to the above, other types of algorithms Ap_i can have a fairly wide range of counteraction At_i. The implementation of countermeasures also depends on:

- the completeness of the information about the identified At_i, which must be in $E_i(At_i)$,
- the type of attack At_i, which has been activated in the object of the attack,
- the way of recognizing At_i for which there is no $E_i(At_i)$ in the *RSB*, and other factors.

A rather large number of scientific and technical publications are devoted to descriptions of attacks and ways to counter attacks of various types [3-5].

Task statement

The purpose of the article is to present the elements of information hazard of an applied task of a distributed information system by a model of sequential processes of impact on incoming, outgoing data, and processes of calculation of the problem.

The article explores ways to use the semantic expert system apparatus to identify inconsistencies (anomalies) in the system based on existing records of incident history and countermeasures.

Lets consider aspects related to enhancing the security of *RIS* (and above all *PSZ* application systems), concerning the problems of countering threats Zg_i and analyzing the hazards Nb_i that Zg_i generates concerning *PSZ*. This raises the following challenges.

1. Analyzing the ability to detect and recognize threats based on attack data that have been activated concerning *PSZ*.

2. Establishing (based on Zg_i data) the possibility of influencing Nb_i by *RSB* means in order to prevent the possible initiation of the process of forming the corresponding threat Zg_i.

3. Analyzing particular aspects of the coexistence of Nb_i, Zg_i, and At_i with *PSZ* objects that may be affected by the eventual retaliatory attacks.

In the paper, by using methods of mathematical logic, the elements of the basic security model to be monitored by RSB are theoretically laid out.

Presentation of the basic material of the study

Most attacks can be considered as $(Pr_i(At_i))$ processes implemented in a certain sequence, and the whole process of attack implementation can be represented at the level of logical implementation At_i. The corresponding processes $Pr_i(At_i)$ can be conventionally considered as realized in steps, which would be considered as elements of the At_i realization process. In this case, it can be written $Pr_i(At_i) = \{l_1, \cdots, l_n\}$, where l_i is a single-step logic realization formula $Pr_i(At_i)$, $l_i = \{x_1 * \ldots * x_k\}$, x_i is a logical variable of the l_i formula, "*" is an arbitrary logical function. When l_i passes to the level of dependencies, at which x_i takes values in the given fields of their definition, l_i passes to the form of analytical, discrete, tabular or other forms of dependencies description, which are interpreted by logical functions, can be written in the form $[l_i = \{x_1 * \ldots * x_k\}] \rightarrow [F_i^t(x_1 \circ \ldots \circ x_k)]$, where «°» are operators, which correspond to the chosen function of dependencies description between x_i and x_j. Let us introduce the notation of additional elements, which are directly related to the elements At_i, Nb_i, and Zg_i. The first of these additional elements are the individual fragments of the object of attack, which are, in the first place, the selected components with *PSZ*, these components will be denoted by the symbol v_i. The next additional element will be a specialist Sp_i in the implementation of unauthorized cooperation with *PSZ* using v_i, which represents the potential opportunity to contribute to the success of the implementation of At_i. Let us assume that the model of Sp_i functioning process is

a system of logical inference $I(L, R)$, where L is a system of logical inference rules, R is a system of heuristic inference rules, which can be included in the system I, if necessary. Heuristic elements are used in problem solving processes when inference rules of classical inference system (for example, Gentzen's inference system) are not enough for problem solving [6]. In the context of this problem, we will define a heuristic rule as an inference rule or some dependency based on the interpretation of some fragment of the domain which is not shown on the level of logical dependencies, since the corresponding heuristic rules describe individual features of links or dependencies in such a fragment. In this case, we can write down such a formal model of hazard: $Nb_i = [M(Sp_i) = I(L,R,D)]$, where D is the input data used in the given model to realize the processes of its functioning. The result of functioning $M(SP_i)$ is the occurrence of Zg_i or $I(L,R,D) \rightarrow Zg_i$. Proceeding from the given variant of description Nb_i as a model of $I(L,R,D)$, we can state that Zg_i is a certain structure At_i which is created based on the use of logical L and heuristic R rules, in which the description of the purpose of functioning Zg_i is formed, which can be written in the form $Zg_i = A_i(L,R,C)$, where C is the purpose of functioning of At_i. As a result of the functioning of Zg_i, it is necessary to obtain a description of the attack - a software product, which is transferred and activated using v_i, or without v_i directly in *PSZ*. To solve this problem, a library of known software implementations of the corresponding types of attacks is used. From the library a program of the corresponding $Ap_i(At_i)$ algorithm and features of its implementation is selected, which has the closest target C_t^* in relation to the target C_i, which is formed in the Zg_i. Based on the determination of the difference between the targets C_t^* and C_i, the necessary modification of the corresponding program is formed. Thus, Zg_i, forms the attack, which, based on the data on *RSB* and v_i, is transmitted to *PSZ* in the form of software implementation of At_i, which is activated. In this case, we will consider the stage of attack object analysis, which is implemented by Zg_i to obtain information about the relevant v_i in order to identify vulnerable points.

In most cases the Nb_i and Zg_i functions are implemented by the corresponding Sp_i specialists. But, in the case of the need to work with distributed systems, which include a large number of individual v_i, it is necessary to automate the relevant processes. Nb_i and Zg_i systems can be considered as objects of influence, which is carried out by means of protection and countermeasures against attacks. Means of protection should prevent the occurrence of attacks [5, 7]. To do this, the following tasks must be solved. Revealing the possibility of an attack by Nb_i, Zg_i and identifying signs of *PSZ*, which may indicate that the attack will occur.

1. Determining the inevitability of an attack in case of Zg_i initiation.

2. Calculating how many and under what conditions different attacks may occur in relation to v_i if Zg_i is initiated by Nb_i danger.

As part of the experiment we will conduct a theoretical analysis of the possibility of obtaining the information needed to solve the problems of counteraction Zg_i. This requires to obtain data on the identified attacks, to determine the causes of their occurrence in order to eliminate (to a greater or lesser extent) the corresponding causes and to counteract the threats that cause the possibility of attacks in the form of dangerous programs and other factors that can lead to disruption of *PSZ* processes. Obviously, it is quite difficult to cover all possible causes of At_i or Zg_i, focused on the implementation of the negative impact on the *PSZ*. Therefore, let us limit ourselves to the functional space of *PSZ*, reflecting the goals of the creation of the corresponding *PSZ* and its interaction with the subject area of interpretation of the corresponding $W_i(PSZ)$ system.

Definition 1. The external environment of the $W_i(PSZ)$ system is all digital media that have direct access to the *RIS* system, regardless of the type of communication channel.

The $W_i(PSZ)$ interpretive domain will be called the external environment *PSZ*. The $W_i(PSZ)$ environment, which we will denote by $H(W_i)$, can be of the following types:

1) an environment $H(W_i)$ that uses information obtained from the *PSZ* system in its processes, we will call a *passive environment* $H^P(W_i)$.

2) The environment $H(W_i)$, which cooperates with *PSZ* by forming information presented to the inputs of *PSZ*, and uses the corresponding results received from *PSZ* to implement its external processes, will be called an *active environment* $H^A(W_i)$.

The corresponding system of processes functioning in W_i we will denote by V^ASZ and V^PSZ and call their external task systems. Assume that the *RIS* system, together with *RSB*, is *PSZ* friendly. Therefore, we can assume that an arbitrary Zg_i (*PSZ*) can occur only in $H(W_i)$. Let us consider statements concerning threats and hazards associated with passive and active external task systems.

Assertion 1. Threat Zg_i (*PSZ*) can arise and exist only in environments V^ASZ, V^PSZ.

Suppose that some Zg_i (*PSZ*) has arisen outside W_i (*PSZ*). Since the W_i (*PSZ*) environment is closed and complete, any Zg_i (*PSZ*) that originated outside $H^P(W_i)$ or $H^A(W_i)$ must interact with W_i(*PSZ*). For *IS*, the functioning of any negative processes is realized by activating the intrusion algorithms (Ar_i) and using information access channels to *PSZ*.

If Zg_i (*PSZ*) does not enter $H(W_i)$, then for Zg_i (*PSZ*) to enter $H(W_i)$, as some intrusive $Ar_i(An_i)$, the latter must have access to the channel of communication with objects with $H(W_i)$. But $H(W_i)$ is a closed environment, which means that $H(W_i)$ provides access only in cases of authorized extension of $H(W_i)$ or in cases where An_i occurs in $H(W_i)$ itself. Since An_i is formed in Nb_i, which is included in $H(W_i)$, and the latter is closed, this contradicts the assumption that Zg_i (*PSZ*) has access to $H(W_i)$. In the case where $H(W_i)$ is extended by some fragment of h_i э $H(W_i)$, the $H^P(W_i)$ and $H^A(W_i)$ systems must identify the corresponding fragment of $h_i(W_i)$ before such an extension can activate its $Pr_i[h(W_i)]$ processes. $H(W_i)$ is friendly to *RIS* and *PSZ*. Thus, if $h_i(W_i) \rightarrow \neg H(W_i)$, then $h_i(W_i)$ is identified as $Ar_i(An_i)$, which confirms that the statement is correct.

Let us consider the case when the information contradiction σ^I between $W_i(VSZ)$ and *PSZ* occurs, which we formally write in the form $\sigma^I[W_i(VSZ)\&PSZ] \geq [\sigma^I(\delta a_i)]$, where δa_i is some threshold value of the contradiction σ^I. Informational contradiction σ^I is the most general type of contradictions because it can include contradictions: logical σ^L, structural σ^S and semantic σ^C.

In order to find the σ^I contradiction dimension it is used the means that determine the degree of consistency of the information received from *RIS* with the information expected by the user, the role of which is almost increasingly played by a separate information system, which we will denote by $P_i(EP)$ symbols. An example of such a mechanism for determining $\sigma^C[PSZ, P_i(Ep)]$, where $P_i(EP)$ э W_i, can be the use of representations of the magnitude of the semantic significance of the two corresponding components [8]. For example, a logical contradiction is defined based on the use of known representations of it from mathematical logic, if the objects concerning which it is defined are descriptions at the level of their logical interpretation [8].

Assertion 2. Nb_i (*PSZ*) hazards can form as a result of contradictions between *VSZ* and *PSZ*.

The notion of Nb_i is always associated with certain contradictions between Nb_i and the object towards which it is directed. In general, Nb_i is essentially a contradiction in relation to the object of influence, which in this case is *PSZ*, which can be written in the form of

$$\{\sigma^I[PSZ, P(EP)] \geq \delta(\sigma^I)\} \rightarrow Nb_i(PSZ). \quad (1)$$

In many cases it is assumed that $Nb_i(Q_i)$, where Q_i is the object of influence, can arise without $\sigma^I(ZQ_i, Q_i)$ contradiction, but for some other reason, where ZQ_i is an object external to Q_i. Such a premise is overly broad.

Let us assume that relation (1) is a precondition for the emergence of Nb_i. Identification of σ^I is an analysis of the $Pr_i[P(EP), VD]$ process, where *VD* is the input from *PSZ*. The magnitude of the contradiction is determined by implementing a control of the input data resulting from the operation of the $Pr_i[P(EP), VD]$ process. After performing this control, the following types of results can be obtained:

- The $Pr_i[P(EP), VD]$ process completed successfully,
- The $Pr_i[P(EP), VD]$ process did not complete successfully.

In the second case there may be the following results.

- There are deviations in the results obtained *R* caused by the $Pr_i[P(EP), VD]$ process itself.

- deviations in the results are caused by the use of false *VD*, or $Te(Pr_i) \rightarrow [\neg R(Pr_i) \vee \neg R(VD)]$, where *Te* is the process testing.

Under *Assertion 2*, the case of $Te(Pr_i) \rightarrow \neg R(VD)$ is relevant. Since it is assumed that PSZ works correctly, the relation is valid: $VD(PSZ) \rightarrow H(VD)$ if takes place:

$[H(PSZ) \rightarrow H(VD)]\{[P(EP), H(VD)] \rightarrow R[Pr_i[P(EP)]]\} \rightarrow [P(EP) \rightarrow Nb_i(PSZ)]$

The interpretation of the above deduction in bringing *Assertion 2* to the qualitative level is as follows: If $Pr_i(PSZ)$ produces VD_i, or $Pr_i(PSZ) \rightarrow VD_i$ without a $P_i(EP)$ consumer in $W_i(PSZ)$, then in $W_i(PSZ)$ the existence of *PSZ* is invisible. We can write the following relation:

$\{[Pr_i(PSZ) \rightarrow VD_i][P(EP), VD_i]\} \rightarrow \{\neg Pr_i[P(EP)] \rightarrow [P(EP) \rightarrow Nb_i(PSZ)]\}$.

If *PSZ* produces VD_i and there is a *P*(*EP*) using VD_i in $W_i(PSZ)$, then in the case of $\{[P(EP), VD_i]\} \rightarrow \neg Pr_i[P(EP)]$, there is a $P(EP) \rightarrow Nb_i(PSZ)$ relation, which proves the statement.

The important task is to determine whether $Zg_i(PSZ)$ can occur when there is a Nb_i hazard in $H(W_i)$. An arbitrary hazard represents some object or process, or other factor, which, by its nature, should not be intended to create threats to objects that may be in its environment. It is reasonable to regard Nb_i as some factor within the framework of such interpretations:

1. Nb_i hazards are created artificially, or under the influence of natural factors in a way that causes the possibility of adverse effects on objects in the environment.

2. Some object Q_i, which is formed artificially from the hazards, may be, in terms of processes of its functioning $Pr_i(Q_i)$, incompatible with the already existing objects of the general environment.

Conclusions

It follows from the above that the presence of Nb_i is caused not so much by the nature of the factors taken separately, as by the negative nature of the possible interaction of Nb_i with the potential ExQ_i objects of its environment. The emergence of Nb_i in $H(W_i)$ can be described as follows: $[(Q_i) \rightarrow \neg(PSZ)] \rightarrow Pr_i(Q_i) \rightarrow Nb_i$. The above relation reflects the conditions for the existence of Nb_i on the binary level. Since there is a task to provide transformations $Pr(Q_i) \rightarrow Nb_i$, in order to use a binary interpretation the process and must be divided into separate components and provided them with an appropriate interpretation. Therefore, let us assume that the following takes place:

$Pr_i(Q_i) \rightarrow Ea[Pr_i(Q_i)] \rightarrow Ed[Pr_i(Q_i)] \rightarrow Er[Pr_i(Q_i)] \rightarrow Nb_i$

where *Ea* is a stage to arise, *Ed* is a stage to develop, *Er* is a stage to ripen. The introduction of such stages requires the identification of attributes or ranges of values of parameters that characterize the corresponding stage of the $Pr_i(Q_i)$ process. The allocation of the corresponding stages can be realized based on the analysis of each type of $Pr_i(Q_i) \rightarrow Nb_i(PSZ)$. In this case different $Pr_i(Q_i)$ at different stages can be combined into separate classes. The emergence of different stages in $Pr_i(Q_i)$ may not mean that the corresponding $Pr_i(Q_i)$ will lead to the emergence of Nb_i.

Let us assume that the emergence of different stages of $Pr_i(Q_i)$ is associated with changes in the values of contradiction between $Pr_i(Q_i)$ and $Pr_i(PSZ)$. Therefore, it is necessary to consider ways of determining the different levels of contradiction $\sigma(Q_i, PSZ)$.

The first level of contradiction σ_1 corresponds to a situation when the use of a result of $Pr_i(Q_i) \rightarrow R_{fi}(Q_i)$ functioning in $H(W)$ does not cause disturbances in $Pr_i(PSZ)$, and the contradiction appears in the occurrence of information redundancy within $Pr_i(PSZ)$ due to the transfer to $Pr_i(PSZ)$ of a result of $R_{fi}(Q_i)$, or:

$\{[Pr_i(Q_i) \rightarrow R_{fi}(Q_i)] \& [R_{fi}(Q_i) \rightarrow Pr_i(PSZ)]\} \rightarrow [Pr_i(PSZ) \leftrightarrow Pr_i(PSZ, R_{fi}(Q_i))]$.

This measure of $\sigma^a(Q, PSZ)$ corresponds to the situation when the presence in Pr_i (*PSZ*) of the result of $R_{fi}(Q_i)$ functioning $Pr_i(Q_i)$ does not lead to changes in the process of functioning of the potential *P*(*EP*) consumer due to his use of the received result of $Pr_i(PSZ)$ functioning.

The second level of contradiction σ_2 corresponds to a situation where the use in Pr_i (*PSZ*) of the result of $R_{fi}(Q_i)$ functioning leads to the formation of data in Pr_i (*PSZ*) that are different from those expected by the *P*(*EP*)

user, but they are non-critical or do not lead to negative consequences of *P*(*EP*) functioning.

The third level of contradiction σ_3 corresponds to a situation where the use in Pr_i (*PSZ*) of $R_{fi}(Q_i)$ results leads to the formation of data in Pr_i (*PSZ*) that are unacceptable, or critical for *P*(*EP*), but their use in Pr_i (*PSZ*) does not lead to unacceptable changes in Pr_i (*PSZ*); this situation is interpreted as the occurrence of Nb_i.

The fourth level of contradiction σ_4 corresponds to the situation when the use in Pr_i (*PSZ*) of the results of $R_{fi}(Q_i)$ causes disastrous consequences in Pr_i (*PSZ*), because in this case the danger is formed.

In the framework of the formulated problem it is proposed to consider the processes connected with the interaction of external objects *Q* with Nb_i as separate stages, and also different levels of contradictions are introduced, which are the main signs of the possibility of occurrence of dangers and threats Nb_i and Zg_i.

The concept of adaptive approach to building an information security system so far raises the question of contextual access to resources and continuous monitoring of information system security indicators, but does not answer what processes and indicators of information system state should be checked [1, 9]. This paper proposes formal markers for monitoring the state of security and protection of an information distributed system.

Prospects for future developments

Information security systems are no longer capable of operating protection perimeters and modeling breaches based on perimeter crossing by unauthorized users or software [10].

Actual today is: monitoring of anomalies, threats, attacks, countermeasures, formation of reference knowledge bases based on the analysis of contradictions in the system of applied tasks, stages of development of threats, attacks within specific resources, actions of users (personified or individual information systems) [11,12]. The paper outlines a formalized basis of parameters for assessing anomalies in distributed systems.

The models of applied task processes, environment, hazards, threats, attacks, anomalies, and contradictions of distributed system objects functioning are proposed. The theoretical foundations of using a semantic analysis expert system to monitor anomalies, determine deviations from standards, form new knowledge base images of threats, attacks, countermeasures are highlighted. In the future, the proposed methods can be applied in the development of software for monitoring and protection of distributed information systems. The experience of using a semantic expert system to analyze and use the knowledge accumulated by IDS/IPS systems is of interest. The results of the study can be used in the construction of fuzzy rules of relationships of vulnerabilities, threats, attacks, countermeasures, consequences for further use of fuzzy logic apparatus of information security risk management.

References

1. Risk Adaptive Approach, Gartner. (2018). https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/Forcepoint/Forcepoint-1-4YCDU8P.pdf.
2. Joint Task Force. (2018). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2.
3. Lukatsky, A. I. (2001). Detection of attacks. SPb.: BHV-St-Petersburg, 624. (In Russian)
4. Zaytsev, O. I. (2006). ROOTKITS, SPYWARE/ADWARE, KEYLOGGERS & DACKDOORS: detecting and protecting. SPb.: BHV-St-Petersburg, 304. (In Russian)
5. Guide for Conducting Risk Assessments. (2012). NIST SP 800-30, Rev. 1. National Institute of Standards and Technology. September, 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.
6. Kleene, Stephen. (1973). Mathematical Logic : monogr. Moskva: Mir, 1973. (In Russian)
7. IOTW: World's Third Largest Music Company Falls Prey To Magecart Attack. (2020). 2020/11/09, 1–2. https://www.cshub.com/attacks/articles.

8. Korostil, Olga, Korostil, Yurii. (2015). Usin text models in systems of control of social objects. Scientific Journals Maritime University of Szczecin: Akademia Morska w Szczecinie, 42(114), 112–117. ISSN 1733-8670.
9. Common Criteria for Information Technology Security Evaluation. (2017). CCMB-2017-04-001. https://www.commoncriteriaportal.org/files/ccfiles /CCPART1V3.1R5.pdf.
10. Zagorodnyy, A., Borovska, O., Svistunov, S., Sinitsyn, I., Rodin, Y. (2014). Creation of an integrated information resource protection system in the national grid infrastructure. Kyiv: Stal, 373. (In Ukrainian)
11. CISO Strategies & Tactics For Incident Response. (2020). August, 2020, 7–11. https://www.cshub.com/executive-decisions/reports/ciso-strategies-tactics-for-incident-response.
12. Scott, Rose, Oliver, Borchert, Stu, Mitchell, Sean, Connelly. (2020). Zero Trust Architecture. NIST Special Publication 800-207. August, 2020, 6–35. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

Received: 30.04.2021

About authors:

Rodin Eugene
junior researcher
The number of articles in the national database – 5
ORCID: https://orcid.org/0000-0003-2416-8572

Sinitsyn Igor
chief of department

The number of articles in the national database – 80
ORCID: https://orcid.org/0000-0002-4120-0784

Affiliation:

Institute of Program Systems of the National Academy of Sciences of Ukraine.
Academician Glushkov Ave., 40, building 5, Kyiv, Ukraine, 03187
(044) 526-55-07, +380674070962
E-mail: yevheniy.s.rodin@gmail.com

Institute of Program Systems of the National Academy of Sciences of Ukraine
Academician Glushkov Ave., 40, building 5, Kyiv, Ukraine, 03187
(044) 526-41-08, +38067-2261313
E-mail: ipsinitsyn@gmail.com