METHODOLOGY OF SECURITY ASSESSMENT AUTOMATED SYSTEMS AS OBJECTS CRITICAL INFORMATION INFRASTRUCTURE

Butusov I.V[1]., Romanov A.A[2].

Abstract. *The technique of estimation of protection of critically important properties of the automated systems as objects of critical information infrastructure is offered. Privacy, integrity and availability of protected resources with different categories of importance are identified as critical properties. It is shown that the existing models of information security systems as part of automated systems and methods for assessing the security of critical properties do not fully reflect the specifics of information security systems as complex organizational and technical systems, the behavior of which, as a rule, reflects the dynamics of poorly structured processes, characterized by a high degree of uncertainty due to non-stationarity, inaccuracy and insufficiency of observations, fuzzy and unstable trends. The reliability of estimates of resource security of automated systems significantly depends on the selected model of formation of the structure of the information security system. Most effective way to increase the reliability of estimates of security is the distribution model of protection mechanisms in the neutralized threats. The statement and the scientific problem of estimation in the conditions of high uncertainty of protection of resources of the automated systems from violations of its critical properties – confidentiality, integrity and availability of the protected resources with various categories of importance is resulted. Determined constraints and assumptions for the task. On the basis of the model of formation of structure of information security system of automated systems by distribution of protection mechanisms on neutralizable threats of information security the values of potential risk from realization of actual threats are determined for each level of protection. The technique is used in the design and development of automated systems of state and military administration.*

Keywords: *critical properties, protected resources, protection mechanisms, fuzzy, uncertainty, levels of protection, threats to information security.*

DOI: 10.21681/2311-3456-2018-1-2-10

Introduction

Automated systems used for the purposes of state administration, defense and security of the country are assigned in accordance with the Federal law No. 187-FZ «on the security of the critical information infrastructure of the Russian Federation», which entered into force on January 1, 2018, to the objects of the critical information infrastructure of Russia. The stability and security of their work are critical to the normal functioning of the state.

The law regulates the procedure for preventing computer incidents at the facilities of Russia's critical information infrastructure and allows us to significantly reduce the negative consequences for our country in the event of computer attacks against it.

In most countries requirements for information security critical information infrastructure are mostly of a voluntary nature, but in connection with the increasingly active terrorist groups using cyber-attacks, the nature of these claims is gradually shifting towards mandatory [1] legislation in combating cybercrime and protecting critical infrastructure are becoming tougher all over the world.

Safety in accordance with Federal law No. 187-FZ is defined as the state of security of critical information infrastructure to ensure its stable operation when carrying out against its attacks.

In automated systems, information security threats are protected by software and hardware environments, implemented on its basis, the applied functionality (business processes) that allows you to accumulate, store and process information, data and information (all together hereinafter-the protected resources) in accordance with the business processes of the system. Security mechanisms as part of information security systems should ensure such critical properties of protected resources as confidentiality, integrity and accessibility.

The high level of risk from the impact of information security threats will be determined in such systems by the use of commercial software, including foreign production, including unlicensed and non-certified software [2], the absence of software updates in the form of patches. In such cases, the threat is neutralized partially or completely through the use of additional measures and protection

1 Igor Butusov, Head of Research Department JSC «Concern SYSTEMPROM», Moscow, Russia. E-mail: butusigor@yandex.ru

2 Aleksandr Romanov, Dr. Sc., Chief specialist JSC «Concern SYSTEMPROM», Moscow, Russia. E-mail: ralexhome@yandex.ru

mechanisms, which, in turn, requires certain financial costs. It should also be noted that the assessment of the security of automated systems as objects of critical information infrastructure significantly depends not only on the number of security mechanisms used as part of information security systems, but also on the degree of confidence in them, as well as on the model of information security system used [3,4].

1. Methods for assessing the security of automated systems

Quantitative estimates of the degrees of security of resources of automated systems due to its strong uncertainty are based, as a rule, on the ratings, which take into account the distribution of protection mechanisms by levels of the hierarchical model of the information security system and the change in the probability (degree) of an attacker achieving the protected resource depending on the level of the model [5].

Two stages can be distinguished in the procedure of evaluating the security of automated systems resources [6,7].

The first stage involves the determination of the effectiveness of potential security provided by individual protection mechanisms, which differ in terms of quality of protection, the presence or absence of FSTEC and/or FSB certificates, the degree of trust, the cost of implementation and operation, etc.in other words, some private performance criteria, on the basis of which protection mechanisms are ranked according to the level of protection that they are able to provide [6.8].

At the second stage, the problem of direct formation of the structure of the information security system is solved. Different sets of mechanisms and methods of protection can be used to neutralize the same threats to information security. The result of solving the problem of forming a rational composition (formation of a rational structure) of the information security system should be an increase in the protection of resources of the automated system.

In well-known studies, for example, [3,9], there are selected set, structural and business process models of information security systems with specified sets of security mechanisms.

In the set models, the effectiveness of protection of automated systems resources is estimated under the assumption that all protection mechanisms are equivalent and participate in the neutralization of threats. To determine the rating of resource security of the automated system, the ratings of durability of individual protection mechanisms are summed up:

$RS = \sum_k rt_{mz_k}$, where rt_{mz_k}- rating of resistance k-th security mechanism.

Structural models of information security systems take into account structural (architectural) features of the system, for example, such as the availability of security tools at 1) hardware level, 2) BIOS level (Basic input-output system), 3) operating system, 4) network level, 5) levels of database management systems and 6) application software.

In the presence j of levels in the system of protection of information and the number k various protection mechanisms mz_k the matrix of resistance ratings of the following type is formed: $M = \{rt_{ij}\}$. Here, each column j of the matrix corresponds to the level of information security system. The matrix element rt_{ij} is equal to 0, if the mechanism of protection i is absent at the level j of information security system. It is assumed that the threat with a certain probability p_j to be neutralized by some mechanism of protection i at the level j of the information security system.

If the n – number of threats, i – number of protection mechanisms, and $n > i$, the probability that a threat from a variety of known threats will be neutralized by a defense mechanism i will be defined as $P_j = i_j / n_j$, where i_j- the number of protection mechanisms, and n_j – the number of threats that are relevant to system-level j data protection.

For each subsequent level of the information security system, the number of actual threats will decrease, as some of them will be neutralized at previous levels of the information security system $n_j = n_{j-1} - i_{j-1}$

Assuming that at all levels the number of protection mechanisms is the maximum possible and the probability of neutralizing the threat at each subsequent level of the information security system will be greater than at the previous level. The vector of distribution of probability of neutralization of threats on levels of system of protection of information is formed: $P = \{P_1, P_2, ..., P_j\}$

The protection matrix Z is formed by multiplying the rows of the resistance rating matrix $M=\{tr_{ij}\}$ on the probability distribution vector $P = \{P_1, P_2, ..., P_j\}$:

$$Z = \begin{Bmatrix} rt_{11}P_1, rt_{12}P_2, ..., rt_{1j}P_j \\ rt_{21}P_1, rt_{22}P_2, ..., rt_{2j}P_j \\ ..... \\ rt_{i1}P_1, rt_{i12}P_2, ..., rt_{ij}P_j \end{Bmatrix},$$

and the rating of protection of system resources is determined by the sum of the matrix elements of security $Z : RS = \sum_i z_i$.

The proposed assessment of the security of resources of the automated system allows to present the results of the analysis of security in quantitative form, which ensures the use of the rating indicator as a target function for optimizing the distribution of security mechanisms by levels of the information security system (criterion – maximizing the rating RS).

The disadvantages of the considered model are the static nature of the system resource security assessment, which does not take into account such parameters as the damage from the implementation of information security threats and the frequency of attacks. In addition, the assumption of reducing the number of actual threats as they approach the object of protection is not always fair (for example, for internal attempts of unauthorized access [5].

In the work [10] security is estimated on the basis of damage from realization in the automated system of the threats having casual character which is estimated through danger factors of threats. Moreover, the hazard factors are represented by fuzzy values, and the indicator of the system security is determined by the method of expert evaluation of the matrix of fuzzy relations between the hazard coefficient of the set of threats and the degree of protection of the resources of the automated system. The disadvantage of such evaluation is the lack of binding of security indicators to the location of security mechanisms in the structure of the information security system. As in the previous case, there is a static evaluation of the security of resources of the automated system.

In [5] is proposed for damage assessment in case of realization of threats to security of information to take into account the expense, in monetary terms, and intangible damage to reputation, competitive advantages of the business entity.

In business process models, the target protected resource is the business processes of an automated system to ensure their continuous functioning in terms of information security threats, which makes it possible to consider the organization of system security in a comprehensive manner, taking into account its architectural and functional features, assessing the adequacy of the planned to use protection mechanisms taking into account the structure of the information security system, to determine metrics and the target security level for the protected resource [9.11].

The paper [12] proposes a risk-oriented approach, according to which risk values from loss of confidentiality, integrity and availability of protected resources are determined separately. The sum of the risk values associated with the loss of certain critical properties will be the total risk:

$$R = P_c \times I_c + P_i \times I_i + P_a \times I_a,$$

where P_c, P_i, P_a – the probability of violation of confidentiality, integrity and availability of protected resources, respectively; I_c, I_i, I – he values of the damage that occurs when the privacy, integrity and availability of protected respectively.

Usually, risk assessment first determines the list of actual threats, and vulnerabilities only characterize the possibility of their implementation. In the present method, the emphasis is shifting from threats to vulnerabilities. Instead of the probability of threats is determined by the probability of vulnerability exploitation, which takes into account both the probability of a vulnerability and the likelihood of its use at least one of the threats.

The fact of realization of information security threat does not necessarily entail violation of critical properties of protected resources. Therefore, for each threat, the probability that its implementation will lead to violation of the critical properties of the protected resources is determined. It is believed that threats to the security of information are independent of each other, so the emergence of one of them does not necessarily lead to the emergence of others. Taking this into account, the following solutions are proposed to calculate the probability of violation of the critical properties of protected resources in [12]:

$$P_c = (1 - \prod_1^n (1 - P_e^j \times P_c^j),$$

$$P_i = (1 - \prod_1^n (1 - P_e^j \times P_i^j),$$

$$P_a = (1 - \prod_1^n (1 - P_e^j \times P_f^j),$$

where P_e^j – the probability of occurrence of the j-th information security threat-the number of vulnerabilities.

In the proposed approach, the calculated risks of violation of critical properties are determined using the concept of «probability», which, as already mentioned, in conditions of high uncertainty seems problematic, as well as the risks are not distributed across the levels of protection of the automated system, the categories of importance of protected resources are not taken into account. In other words, system security assessments are not tied to the information security system model.

Modeling the structure of the system of information security and assessment of the level of security

of automated system – a necessary step for automation of procedures for the analysis of vulnerabilities and detection of attacks on a system with the objective of making the protection systems information on the evolutionary properties of adaptability and development [13].

Existing models of information security systems as part of automated systems and methods for assessing their security do not fully reflect the specifics of information security systems as complex organizational and technical systems, the behavior of which, as a rule, reflects the dynamics of poorly structured processes characterized by a high degree of uncertainty due to non-stationarity, inaccuracy and insufficiency of observations, fuzzy and unstable trends [11,14]. These models and methods mainly use statistical interpretation of quantitative estimates, for example, using the concept of «probability», which, with undeniable advantages and wide recognition of the statistical approach, limits the use of the existing conceptual apparatus in the creation of information security systems and resource security assessment of automated systems with designated properties. In addition, statistical models do not provide fuzzy (linguistic) interpretation of data and results, and in modern conditions this quality of models is demanded by experts in the field of information security and it is necessary for systems of intellectual analysis, operating with fuzzy values. Thus, the analysis of the above methods of evaluation of security of automated systems and models of formation of information security systems shows the theoretical and practical relevance of solving the scientific problem of evaluation in conditions of high uncertainty of security of automated systems against violations of its critical properties – confidentiality, integrity and availability of protected resources with different categories of importance. The solution of the problem of assessing the security of automated systems should be made on the selected model of the formation of the structure of the information security system, taking into account the particular criteria for the effectiveness of individual protection mechanisms, the relationship with the integral requirements (criteria) of the security of specific systems in terms of the integrity, availability and confidentiality of protected resources, as well as the indirect relationship of threats to information security neutralizing their protection mechanisms through private performance criteria.

2. The choice of the model of formation of structure of system of protection of information and the problem statement evaluate the security of automated systems

2.1. The choice of the model of formation of structure of information security system

In automated systems, software and hardware environments are protected against threats to information security, as already mentioned, implemented on its basis the applied functionality (business processes), which allows to accumulate, store and process information, data and information in accordance with the business processes of the system [9.11]. Security mechanisms as part of an information security system should provide critical features of protected resources with different categories of importance, such as confidentiality, integrity and accessibility.

Neutralization of current threats to information security is carried out at several levels of system protection: BIOS (Basic input-output system), hardware, operating system, network, database management system, functional (applied) software. Known methods, for example, [3], the formation of the structure of the information security system, as a rule, solve the problem of forming optimal sets of protection mechanisms without taking into account the architecture of the automated system, which should correspond to the structure of the information security system. Therefore, the optimality of such sets does not yet indicate the optimality of the sets of protection functions from these levels involved in neutralizing a specific threat to information security.

The model of information security system should have the property of adaptation to neutralizable threats or, in other words, the problem of rational distribution of protection mechanisms on neutralizable threats to information security should be solved in the model.

From the scientific literature the method of distribution of protection mechanisms on neutralizable threats to information security in the hierarchy of protection levels compared to the architecture of the automated system is known [15].

The distribution of protection mechanisms for neutralized threats in accordance with the methodology is based on multiple partial criteria of efficiency that are applicable to the protection mechanisms, and neutralized threats. Such criteria include, for example, the cost of protection functions/the cost of neutralizing an actual threat (criterion kr_1); the weighted average number of threats neutralized by a protection mechanism/ the weighted average number of protection mechanisms neutraliz-

ing an actual threat (criterion kr_2); the magnitude of the vaccine-preventable mechanism of protection of risk from the implementation of the actual threat/value of preventing the risk of realization of threat (criterion kr_3); the degree of confidence in the mechanism of protection/degree of confidence in the protection mechanism against the escape of threats (criterion kr_4) [16]; the degree of compatibility of mechanisms of protection/degree of compatibility of the protection mechanisms against the threats neutralized (criterion kr_5).

The application of this technique is effective even if updates in the form of software patches are not made in the HS as, and the neutralization of threats is partially or completely carried out through the use of additional measures and protection mechanisms, which, in turn, requires certain financial costs.

The results of the application of the method formed subsets $M_n = \{mz_{ku}\}$ protection mechanisms mz_{ku} most effectively neutralizing the threat ug_n at the levels of protection $ur_u \in UR$. Here $n = \overline{1,N}$ – the number of actual threats to information security, $u = \overline{1,U}$ – many levels of information security, $k = \overline{1,K}$ – the number of protection mechanisms.

With such a model of building an information security system as a result of solving the problem of assessing the security of automated systems from violations of its critical properties – confidentiality, integrity and availability of protected resources, you can get the most reliable results. And protected resources can have different categories of importance, in particular, particularly important, very important, important or unimportant, reflecting their value in the business processes implemented by the system.

2.2. Problem statement

Let $M_n=\{mz_k\}$ – subsets formed by the method of distribution of protection mechanisms on neutralizable threats to information security. These subsets include protection mechanisms mz_k that most effectively neutralize actual threats $ug_n \in UG$, $n = \overline{1,N}$, N – the number of actual threats to information security; $k = \overline{1,K}$ – the number of protection mechanisms [15].

Protection mechanisms are divided into levels of protection, $ur_u \in UR$, $u = \overline{1,U}$, U – the number of levels of protection, $MZ = \{mz_k\} = \bigcup_{u=1}^{U} MZ_u = \{mz_{k \in K_u, u}\}$, where MZ_u – a subset of the mechanisms of protection level $ur_u \in UR$, $k \in K_u$ – is a subset of the indices of protection mechanisms on this level, $\bigcup_u K_u = K$, $\bigcap_u K_u = \varnothing$.

The threat ug_n is represented as a vector $ug_n = \{p^{ug_n}, uch^{ug_n}, rsk^{ug_n} = p^{ug_n} \times uch^{ug_n}\}$ [3.15], where p^{ug_n} – assessment of the possibility of a threat ug_n, uch^{ug_n} – damage from the implementation of the threat ug_n, rsk^{ug_n}– the risk from the implementation of the threat ug_n.

The sets $zr_z \in ZR$ of protected resources of the information system are defined, $z = \overline{1,Z}$, Z – the number of protected resources, and the degrees of value (categories of importance) $KV = \{kv_v\}, v = \overline{1,V}$ that can be assigned to protected resources.

It is necessary to form assessments of automated system security based on risks from privacy violations, integrity and availability of protected resources with different categories of importance, both individually, including security levels, and for the system as a whole.

2.3. Limitations and assumptions

The scientific literature and standards usually consider a three – level approach to risk assessment-the level of information systems, the level of business processes and the organizational level [12]. At the system level, the list of protected resources, vulnerabilities and threats to information security, as well as the measures and mechanisms of protection are determined. This information is sufficient to determine the possibility of damage. The value of the protected resources and, accordingly, the amount of damages to be determined primarily at the level of the business processes and the organizational level with the involvement of the owners of the business processes, management and other stakeholders. In the present paper we do not aim to determine the amount of damage from the violation properties of the protected resource, allowing you to analyze only the level of the automated system with corresponding structure information. Damage is understood as harm, losses, damages caused to the system and may lead to inability to perform or improper performance of its functions and/or not to achieve the objectives of the system without additional costs of material, labor and/or other types of resources [12].

Risk values from loss of confidentiality, integrity and availability of protected resources will be determined separately. Let us also assume that threats to the security of information arise independently of each other and therefore the occurrence of one of them does not necessarily lead to the emergence of others. Implementation of a threat does not always entail a violation of the critical properties of protected resources and therefore for each threat it is necessary to determine the degree of possibility that its

implementation will lead to violation of the critical properties of protected resources.

Calculation of the degree of the possibility of violation of the critical properties of protected resources will take into account the maximum possible implementation of threats, and the full risk to the automated system will be defined as the maximum risk of violation of the critical properties of protected resources.

3. Evaluate the security of automated systems

3.1. Assessment of the degree of neutralization mechanisms for the protection of actual security threats

As you know, the attack potential is estimated according to the same scheme as the degree of risk from the presence of vulnerabilities, but with some differences (for example, from several attack scenarios selected the worst, with the greatest potential). It is believed that it is a function of the level of motivation of the attacker, his skills and available resources. Motivation affects allocated to time attack and possibly attract resources and recruitment of attackers [5].

Then the degree $\mu_{\tilde{A}_i^{kvk}}(mz_k)$ of neutralization of the threat ug_i by the protection function mz_k can be determined as follows:

$$\mu_{\tilde{A}_i^{kvk}}(mz_k)=\begin{cases}1, & \text{если } r_c^{kvk}\ge r_н^{kvk};\\ \dfrac{r_c^{kvk}}{r_н^{kvk}}, & \text{если если } r_c^{kvk}<r_н^{kvk}\end{cases}..$$

Here r_i^{kvk} – is the ranking of potential attack, r_c^{kvk} – rating durability protection features, and $kvk=\{knf,cls,dst\}$ – many designations of critical criteria for: knf –– confidentiality, cls – integrity and dst – availability. $\tilde{A}_i^{kvk}$ – an fuzzy subset of protection mechanisms mz_k that can neutralize a threat ug_i^{kvk} designed to violate one of the critical criteria, $i=\overline{1,N}$ – the number of actual security threats.

According to the method of distribution of protection mechanisms for the escape threats of a fuzzy set $\tilde{A}_i^{kvk}$ can be defined by the matrix $M\tilde{G}$:

$$M\tilde{G}=\begin{bmatrix} & \begin{bmatrix} ug_1^{kvk} & ug_2^{kvk} & \dots & ug_N^{kvk}\end{bmatrix}\\ \begin{bmatrix}mz_1\\mz_2\\.\\.\\.\\mz_K\end{bmatrix} & \begin{bmatrix}\mu_{\tilde{A}_1^{kvk}}(mz_1,ug_1^{kvk}) & \mu_{\tilde{A}_2^{kvk}}(mz_1,ug_2^{kvk})\dots\mu_{\tilde{A}_N^{kvk}}(mz_1,ug_N^{kvk})\\ \mu_{\tilde{A}_1^{kvk}}(mz_2,ug_1^{kvk}) & \mu_{\tilde{A}_2^{kvk}}(mz_2,ug_2^{kvk})\dots\mu_{\tilde{A}_N^{kvk}}(mz_2,ug_N^{kvk})\\ . & . \quad . \quad . \quad . \quad . \quad . \quad .\\ . & . \quad . \quad . \quad . \quad . \quad . \quad .\\ . & . \quad . \quad . \quad . \quad . \quad . \quad .\\ \mu_{\tilde{A}_1^{kvk}}(mz_K,ug_1^{kvk}) & \mu_{\tilde{A}_2^{kvk}}(mz_K,ug_2^{kvk})\dots\mu_{\tilde{A}_N^{kvk}}(mz_K,ug_N^{kvk})\end{bmatrix}\end{bmatrix},$$

where

$$\mu_{\tilde{A}_n^{kvk}}(mz,ug_n^{kvk})=\frac{\sum_{kr}\mu_{M\tilde{R}}(mz,kr)*\mu_{K\tilde{G}}(kr,ug_n)}{\sum_{kr}\mu_{M\tilde{R}}(mz,kr)},$$

for all $mz_k\in MZ$, $kr_j\in KR$, $ug_n\in UG$.

The sum $\sum_{kr}\mu_{M\tilde{R}}(mz,kr)$ is interpreted as the number of significant criteria kr characterizing the properties mz_k, and $\mu_{\tilde{A}_n^{kvk}}(mz_k,ug_n^{kvk})$ represents a weighted degree of neutralization of the actual threat ug_n^{kvk} by the protection mechanism mz_k (the degree of preference when choosing a protection mechanism mz_k to neutralize the actual threat ug_n^{kvk}).

The calculated values $\mu_{\tilde{A}_i^{kvk}}(mz_k,ug_i^{kvk})$ reflect the degree of neutralization of the threat ug_i^{kvk} by the protection mechanism mz_k, taking into account the values of the criteria for the effectiveness of protection mechanisms.

At the same time, we believe that for any threat there is a mechanism of protection such that $r_c^{kvk}\ge r_i^{kvk}$: $\forall ug_i^{kvk}\ \exists mz_k \mid r_c^{kvk}\ge r_н^{kvk}$ – any threat is neutralized by at least one mechanism of protection.

For each level of protection $ur\in UR$ using the original matrix $M\tilde{G}$, it is possible to form fuzzy matrices $M\tilde{G}_u$ containing estimates of the degree of neutralization of threats by protection mechanisms from the level of protection ur (for ease of presentation, we will not write indexes indicating critical properties):

$$M\tilde{G}_u=\begin{bmatrix} & \begin{bmatrix} ug_1 & ug_2\dots & ug_{n_u}\end{bmatrix}\\ \begin{bmatrix}mz_1\\mz_2\\.\\mz_{k_u}\end{bmatrix} & \begin{bmatrix}mt_{11} & mt_{12}\dots mt_{1n_u}\\ mt_{21} & mt_{22}\dots mt_{2n_u}\\ . \quad . & . \quad .\\ mt_{k_u1} & mt_{k_u2}\dots mt_{k_un_u}\end{bmatrix}\end{bmatrix},$$

where $mt_{ij}=\mu_{MG_u}(mz_{k_u},ug_{n_u})$, $k_u\in\{K_u\}\subset K$ – the indices of defense mechanisms, included in the protection level ur_u, $n_u\in\{N_u\}\subset N$ – the indices of the security threats relevant to that level.

You can create a fuzzy relationship between current threats and the level of protection at which they are neutralized, $te_{ij}=\mu_{UR_u^{ug}}(ug_i,ur_j)=\max_{k_u}\{\mu_{M\tilde{G}_u}(mz_{k_u},ug_{n_u})\}$ – the degree of neutralization of the threat ug_i at the level of protection ur_j:

$$UR_u^{ug} = TE_{ur} = \begin{bmatrix} ug_1 \\ ug_2 \\ . \\ ug_N \end{bmatrix} \begin{bmatrix} te_{11} & te_{12} & \dots & te_{1U} \\ te_{21} & te_{22} & \dots & te_{2U} \\ & & \dots & \\ te_{N1} & te_{p2} & \dots & te_{NU} \end{bmatrix}, \quad \begin{bmatrix} ur_1 & ur_2 \dots ur_U \end{bmatrix}$$

where $i = \overline{1,N}$ – the number of actual threats, $j = \overline{1,U}$ – the number of levels of protection in the structure of the information security system. In other words, at each level of protection, the mechanism of protection with the maximum degree of its neutralization is chosen to neutralize the actual threat.

In the structure of the information security system at each level of protection can assess the level of potential risk and to form fuzzy relation $RSK_{ug}^{ur} = ET$:

$$RSK_{ug}^{ur} = ET = \begin{bmatrix} ur_1 \\ ur_2 \\ . \\ ur_U \end{bmatrix} \begin{bmatrix} et_{11} & et_{12} & \dots & et_{1N} \\ et_{21} & et_{22} & \dots & et_{2N} \\ & & \dots & \\ et_{U1} & et_{U2} & \dots & te_{UN} \end{bmatrix}, \quad \begin{bmatrix} ug_1 & ug_2 \dots ug_N \end{bmatrix}$$

where $et_{ij} = \mu_{RSK_{ug}^{ur}}(ur_i, ug_j) = uch^{ug_j} \times \times \max_{k_u \in K_u} \{p^{ug_j} \times ((1 - \mu_{MG_u}(ug_j, mz_{k_u}))\}$, $i = \overline{1,U}$ – the number of levels of protection in the structure of the information security system, $j = \overline{1,N}$ – the number of actual threats, $k_u \in K_u \subset K$ – indices of protection mechanisms that neutralize the threat at the level of protection ur_i.

Fuzzy attitude RSK_{ug}^{mz} determines the risk from the implementation of the current threat ug_j.

$$RSK_{ug}^{mz} = TM = \begin{bmatrix} ug_1 \\ ug_2 \\ . \\ ug_N \end{bmatrix} \begin{bmatrix} tm_{11} & tm_{12} & \dots & tm_{1K} \\ tm_{21} & tm_{22} & \dots & tm_{2K} \\ & & \dots & \\ tm_{N1} & tm_{p2} & \dots & tm_{NK} \end{bmatrix}, \quad \begin{bmatrix} mz_1 & mz_2 \dots mz_K \end{bmatrix}$$

where $tm_{ij} = \mu_{RSK_{ug}^{mz}}(ug_i, mz_j) = \max_{i=1}^{N} uch^{ug_\emptyset} \times \times P^{ug_i} \times ((1 - \mu_{MG_u}(ug_i, mz_j))$ – the degree of risk from the implementation of the actual threat ug_j and $i = N$ – the number of known threats-the number of protection mechanisms.

3.2. Assessment of protection of critical properties

Taking into account the accepted restrictions and assumptions, we will assume that the risks of breach of confidentiality RSK_{cnf}, integrity RSK_{cst} and availability RSK_{dst} of protected resources $zr_z \in ZR$, $z = \overline{1,Z}$, z – the number of protected resources are calculated independently of each other, and the total risk is determined as the maximum risk of violation of critical properties:

$$RSK = \max\{RSK_{cnf}, RSK_{cst}, RSK_{dst}\}.$$

Protected resources are assigned the category of importance $\mu_{KV}(zr_z, kv_v))$, $KV = \{kv_v\}, v = \overline{1,V}$, $\mu_{KV}(zr_z, kv_v))$ – the degree of correspondence of the protected resource $zr_z \in ZR$ to the category of importance kv_v.

We also believe that the mechanisms of information protection in the structure of protection systems are designed to protect certain resources, that is determined by the extent to which they are used to protect these resources $\mu_{ZM}(zr_z, mz_k)$. Since the protection mechanisms are designed to neutralize with a certain degree of actual threats to the security of information, the calculation of the degree of violation of the confidentiality of protected resources at each level of protection can be done by the following formula:

$$P_{cnf}^u = (1 - \min_z\{1 - \mu_{KV}(zr_z, kv_v) \times \times (\max_{mz_k} \mu_{ZM}(zr_z, mz_k) \min_{ug_u}(1 - t_{un}) \times P^{ug_n})\}.$$

This and forth $t_{un} = \mu_{MG_u}(mz_{k_u}, ug_{n_u})$ – degree of neutralization of threat ug_n by the mechanism of protection mz_k at the level of protection ur_u, $\min_{ug_u}(1 - t_{un}) \times P^{ug_n})$ indicates the extent to which the threat ug_n is not neutralized by the protection mechanism mz_k at the protection level ur_u. The protection mechanism mz_k is designed to protect a resource zr_z from threats according to attitude TE_{ur}.

The expression $\max_{mz_{kz}} \mu_{KV}(zr_z, mz_k)$ determines the choice of the worst-case scenario when exposed to all possible threats to the protected resource when protected by all possible protection mechanisms.

The expression $sz_{cnf}^u = \min_z\{1 - \mu_{KV}(zr_z, kv_v) \times \times (\max_{mz_k} \mu_{ZM}(zr_z, mz_k) \min_{ug_u}(1 - t_{un}) \times P^{ug_n})$ determines the degree of protection of automated system resources from privacy violations at the level of protection $ur_u \in U$.

In General, for the system, the degree of privacy violation of protected resources is defined as the worst option of all levels of protection – $sz_{cnf} = \min_u\{sz_{cnf}^u\}$.

For threats aimed at violating integrity and accessibility, it is necessary to take into account the indicator $S_{восm.zr}$ – the degree of restoring the integrity (availability) of the protected resource (if the protected resource is not affected or its degree of importance is zero, then this degree is identical to 1):

$$P^{u}_{cst/dst} = (1 - \min_{z}\{1 - \mu_{KV}(zr_z, kv_v) \times (1 - S_{восm.zr_z}) \times$$

$$\times (\max_{mz_k} \mu_{ZM}(zr_z, mz_k) \min_{ug_u} (1 - t_{un}) \times P^{ug_n})\}.$$

Then the expression

$$sz^{u}_{cst/dst} = \min_{z}\{1 - \mu_{KV}(zr_z, kv_v) \times (1 - S_{восm.zr_z}) \times$$

$$\times (\max_{mz_k} \mu_{ZM}(zr_z, mz_k) \min_{ug_u} (1 - t_{un}) \times P^{ug_n})$$

specifies the degree of protection of resources of the automated system from violating the integrity/availability on the level of protection $ur_u \in U$.

For an automated system as a whole, the degree of violation of integrity/availability of protected resources is defined as the worst case of all levels of protection – $sz_{cst/dst} = \min_{u}\{sz^{u}_{cst/dst}\}$. The degree of protection against violation of all critical properties is logical to determine how $sz_{cnf/cst/dst} = \min_{u}\{sz_{cnf}, sz_{cstt}, sz_{dst}\}$.

Conclusions

1. The critical properties of the automated systems as objects of critical information infrastructure can be attributed to the confidentiality, integrity and availability of protected resources with different categories of importance.

2. The reliability of estimates of the security of automated systems depends significantly on the model of formation of the structure of the information security system, which should have the property of adaptability to neutralizable threats to information security.

3. In the known models of formation of the structure of information security systems and methods for assessing the security of resources, mainly used statistical interpretation of quantitative estimates, for example, using the concept of «probability», which, with the undoubted advantages and wide recognition of the statistical approach, makes it difficult to solve the problem of assessing the security of automated systems in conditions of strong uncertainty.

4. The theoretical and practical relevance of the scientific problem of evaluation in the conditions of high uncertainty of automated systems protection against violations of its critical properties – confidentiality, integrity and availability of protected resources with different categories of importance.

5. The reliability of estimates of resource security of automated systems significantly depends on the selected model of formation of the structure of the information security system. Most effective way to increase the reliability of estimates of security is the distribution model of protection mechanisms in the neutralized threats.

6. The statement and the scientific problem of estimation in the conditions of high uncertainty of protection of resources of the automated systems from violations of its critical properties – confidentiality, integrity and availability of the protected resources with various categories of importance is resulted. Restrictions and assumptions for the solution of the task are defined.

7. On the basis of the model of formation of structure of information security system of automated systems by distribution of protection mechanisms on neutralizable threats of information security the values of potential risk from realization of actual threats are determined for each level of protection.

8. The technique of estimation of resources security of the automated systems in General and on levels of protection against violations of its critically important properties is offered.

9. The technique is used in the design and development of automated systems of state and military administration.

***Reviewer**: V.L. Tsirlov, Ph.D., Associate Professor, Information Security Department, Bauman Moscow State Technical University, Moscow, Russia. E-mail: v.tsirlov@bmstu.ru*

References:

1. Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K. Organization of the entrusted calculations in crucial objects of informatization under uncertainty. In Proceedings of the 20th IEEE International Conference on Soft Computing and Measurements (24-26 May 2017, St. Petersburg, Russia). SCM 2017, 2017, pp. 299 - 300. DOI: 10.1109/SCM.2017.7970566.
2. Kuz'min A.S., Romanov A.A. Importozameshchenie: reaktsiya na ugrozy ili osobyĭ tip gosudarstvennoĭ strategii, BIS Journal [Informatsionnaya Bezopasnost' Bankov], 2015, No 2, pp. 16-22
3. Olad`ko V. S. Model' vybora ratsional'nogo sostava sredstv zashchity v sisteme elektronnoĭ kommertsii, Voprosy kiberbezopasnosti [Cybersecurity issues], 2016, No1 (14), pp. 17-23.
4. Yandybaeva é. é., Mashkina I.V. Razrabotka modeli planirovaniya ispol'zuemykh sredstv zashchity informatsii dlya informatsionnykh system élektronnykh torgovykh ploshchadok, Vestnik Ufimskogo gosudarstvennogo aviatsionnogo tekhnicheskogo universiteta. 2015, V. 19, No 1, pp. 264-269.
5. Osovetskiĭ L., Shevchenko V. Otsenka zashchishchënnosti seteĭ I system, ékspress élektronika. 2002, No 2-3, pp. 20-24.

6. Barabanov A., Markov A., Fadin A., Tsirlov V. Statistics of software vulnerabilities detection during certified testing, Voprosy kiberbezopasnosti [Cybersecurity issues], 2018, No 2(20), pp. 2-8. DOI: DOI: 10.21681/2311-3456-2017-2-2-8.
7. Bibashov S.A. Model' formirivaniya trebovaniĭ po zashchite informatsii k zozdavaemŷm avtomatizirovannŷm sistemam v zashchishchënnom ispolnenii, Voprosy kiberbezopasnosti [Cybersecurity issues], 2017, No 5(23), pp. 83-90. DOI: 10.21681/2311-3456-2017-5-83-90.
8. Chabonyan V.A., Shalakhov Yu.I. Analiz I sintez trebovaniĭ k sistemam bezopasnosti ob'ektov kriticheskoĭ informatsionnoĭ infrastrukturŷ, Voprosy kiberbezopasnosti [Cybersecurity issues], 2013, No 1(1), pp. 17-27.
9. Lukinova O.V. Semanticheskoe opisanie faktorov bezopasnosti informatsionnŷkh system pri proektirovanii system zashchity, Sistemŷ vysokoĭ dostupnosti, 2013, No 3, pp. 149-156.
10. Karpŷchëv V.Yu., Minaev V.Yu. Tsena informatsionnoĭ bezopasnosti, Sistemŷ bezopasnosti. 2003, No 5, pp.128-130.
11. Butusov I.,V., Nashchekin P.A., Romanov A.A. Teoretiko-semanticheskie aspekty organizatsii kompleksnoy sisitemy zashchity informatsionnykh system, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2016, No1(14), pp. 9-16.
12. Nurdinov R.A. Opredelenie veroyatnosti narusheniya ktiticheskikh svoĭstv informatsionnogo aktiva na osnove CVSS metric uyazvimosteĭ, Sovremennŷe problemŷ nauki I obrazovaniya. 2014, No 3. Open Access: URL: http://science-education.ru/ru/article/view?id=13290.
13. Borodaky Yu.V., Mironov A.G., Dobrodeev A.Yu., Boldyna M.N. Problemy i perspektivy sozdaniya evolutsioniruyushchikh intellectual,nykh system zashchity informatsii dly sovremennykh raspredelennykh informatsionno-upravlyayushchikh system i kompleksov spetsial,nogo i obshchego naznacheniy//Nauchnye problem national,noy bezopasnosty Rossiyskoy Federatsii. vyp. 5: K 20-letiyu obrazovaniya Soveta Bezopasnosti Rossiyskoy Federatsii, Moscow, Izd-vo Izveatiya, 2001, pp. 303-307.
14. Shcherbakov E.S., Korchagin P.V. Primenenie metodov teorii vozmozhnosteĭ pri modelirovanii sistem zashchitŷ informatsii, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2017, No 1(19), pp. 2-5. DOI: 10.21681/2311-3456-2017-1-2-5.
15. Murzin A.P., Butusov I.V., Romanov A.A. Adaptatsiya sistemŷ zashchitŷ informatsii avtomatizirovannŷkh system upravlrniya k neĭtralizuemŷm ugrozam, Priborŷ i sistemŷ. Upravlenie, rontrol', diagnostika. Avtomatizirovannŷe systemŷ upravlrniya. 2017, No 10, pp. 1–7.
16. Zakharenkov A.I., Butusov I.V., Romanov A.A. Method kolichestvennoĭ otsenki stepeni doverennosti programmno-apparatnŷkh sredstv, Priborŷ i sistemŷ. Upravlrnie, control', diagnostika. Avtomatizirovannŷe sistemŷ upravleniya, 2017, No 8, pp.34-39.