The Method of Allocation of the Security Functions in Neutralized Threats to Critical Information Systems

Igor V. Butusov
Research Department
Concern SYSTEMPROM, JSC
Moscow, Russia
butusigor@yandex.ru

Alexander A. Romanov
Research Department
Concern SYSTEMPROM, JSC
Moscow, Russia
ralexhome@yandex.ru

Abstract – It is shown that the optimality of the feature sets of the protection levels of the information security system for automated systems not yet proves the optimality of these sets to neutralize threats to information security. The proposed method of adaptation of the information security system to escape threats by distributing the security functions to escape many threats on the levels of protection. Justified a hypothesis about the identity of the system evaluation criteria security threats and neutralizing their protection features. The estimates of security and threats to information security, the weighted cost of neutralizing the threats, considered the correctness of the implementation of security functions. Evaluation of the effectiveness of the security functions generated based on a cost average number of neutralized threats, preventable risk, the extent of the power of attorney and compatibility. Quantitative estimates of the values of the performance criteria represented by continuous functions. The input parameters are fixed at the time of the assessment of individual criteria of the efficiency of the security functions. Defined decision rule and the threshold of semantic preference in the allocation of security functions for neutralized threats to information security. Semantic preference threshold is used to select the functions of protection, the most effectively neutralizing the threat to levels of protection in the structure of information security system as a whole. The methodology used in the design, development and maintenance of security systems.

Keywords – information security, security functions, threats, performance criteria, performance evaluation, semantic threshold preferences, degree preference, evaluation level, protection level, decision rule

I. INTRODUCTION

Rational sets of security features are formed using type-setting, structural and business process models of information security systems (e.g. [1-4]) and appropriately documented [5].

The optimality of the feature sets of the security levels of the underlying system input-output, hardware, operating system, network, database management system, application software. still no evidence on the optimality of the sets of security features of these levels are involved in neutralizing specific threats.

Security functions that are distributed throughout the threats of information security needs to ensure their effective neutralization in conditions of strong uncertainty, that the undoubted advantages and the recognition makes it difficult to use statistical (probabilistic) approach.

Urgent becomes the task of developing the methodology for the allocation of security functions for neutralized threats in conditions of strong uncertainty.

II. STATEMENT OF THE PROBLEM

A. Model of information security system

Let be $MOD_{СЗИ} =< \{UR\},\{UG\},\{MZ\},\{KR\},\{TR\} >$ – a model of the system of information protection.

Here $ur_u \in UR$ – levels of protection in the system of information protection, $u = \overline{1,U}$, U – the number of levels of protection; $ug_n \in UG$ – many pressing threats to information security for critical information systems, $n = \overline{1,N}$, N – количество актуальных угроз;

$MZ = \{mz_k\} = \bigcup_{u=1}^{U} MZ_u = \{mz_{k \in K_u, u}\}$, где MZ_u – a subset of the functionality of protection level of protection $ur_u \in UR$, $k \in K_u$ – a subset of the indexes $k = \overline{1,K}$ security features at this level, $\bigcup_u K_u = K$, $\bigcap_u K_u = \varnothing$;

$kr_j \in KR, j = \overline{1,J}$, many criteria for evaluating the effectiveness of the security features;

$tr_{mz_{ku}} \in TR$ – many of the requirements to the security: $tr_{mz_{ku}} = \{rsk^{\partial on}_{mz_{ku}}, st^{\max}_{mz_{ku}}\}$, where $rsk^{\partial on}_{mz_{ku}}$ – the permissible level of risk from the threat is credible, $st^{\max}_{mz_{ku}}$ – the maximum allowable costs for the security function (for a class of functionally similar protection features)..

B. The threat to information security

Threat ug_n we describe the vector $ug_n = \{p^{ug_n}, uch^{ug_n}, rsk^{ug_n} = p^{ug_n} \times uch^{ug_n}\}$ [6], где p^{ug_n} – evaluation of the possibility of a threat ug_n, uch^{ug_n} – the damage from realization of threats ug_n, rsk^{ug_n} – the risk from implementation of threats ug_n.

C. Formation of information security system

Required to form the structure of information security system by distributing $mz_{ku} \in MZ$ many pressing threats to information security $ug_n \in UG$:

$$M_{СЗИ} = \bigcup_n M_n = \{mz_{k1} \mid \max_{k \in K_1} poss(mz_{k1}, ug_n); ...,$$

$$mz_{ku} \mid \max_{k \in K_u} poss(mz_{ku}, ug_n); ...,$$

$$mz_{ku} \mid \max_{k \in K_U} poss(mz_{ku}, ug_n).$$

Здесь $mz_{ku} \mid \max_{k \in K_u} poss(mz_{ku}, ug_n)$ – security functions mz_{ku} index $k \in K_u$ the selected protection level $ur_u \in UR$ to provide maximum ability to neutralize actual threats $ug_n \in UG$.

III. HYPOTHESIS

A. Identity criteria

We believe that actual threats to information security are characterized by the properties inherent protection features, and evaluated on the same criteria, but choosing the worst score for neutralizing their protection features.

B. Justification

Potential attacks are evaluated as a whole according to the same scheme as the risk of the presence of vulnerabilities, but with some differences, for example, of several scenarios of attack is chosen by worst, with the most potential [7]. It is believed that it is a function of the level of motivation of the attacker, his skill and available resources. Motivation affects allocated to time attack and possibly attract resources and recruitment attackers.

Then, the degree of $\mu_{\tilde{A}_i}(mz_k)$ neutralize the threat ug_i security function mz_k you can define as follows:

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

Here $r_н$ – the ranking of potential attacks, r_c - the rating durability protection features. We believe that any threat exists, the security function such that $r_c \geq r_н$: $\forall ug_i \ \exists mz_k \mid r_c \geq r_н$ – any threat neutralised at least one security feature.

IV. PERFORMANCE CRITERIA SECURITY FUNCTIONS

On the sets of actual threats $ug_n \in UG$ and security functions $mz_k \in MZ$ determined attitude MU. In the General case $\mu_{MU}(ug_n, mz_k) \in [0,1]$ – evaluation of the possibility of neutralizing the security function mz_k current threats ug_n.

Evaluation of the effectiveness of the security features is going to be calculated according to the criteria presented below [4, 6, 8]. We believe that the quantitative estimation of the criteria values representable by continuous functions and monotonically vary depending on the input parameters. The input parameters are fixed at the time of the assessment of individual criteria of the efficiency of the security functions.

A. Cost (criterion kr_1)

1) The Cost of security functions. Quantitative assessment criteria can be calculated according to the formula

$$kr_1 = \frac{1}{\left(1 + \left(\dfrac{st_{mz_k}}{a_1}\right)\right)^{b_1}},$$

where $0 < st_{mz_k} \leq st_{mz_k^l}^{\max}$, a_1, b_1 – the configurable settings. As a parameter a_1 it is recommended to select a value $st_{mz_{ku}}^{\max}$ – the maximum allowable costs for the protection feature.

2) The Cost of neutralizing actual threats. Denote by $mz_{ku}(kr_1)$ the value of the criterion kr_1 for security features mz_{ku}. Then the value $ug_n(kr_1)$ criteria kr_1 for threats ug_n defined as follows:

$$ug_n(kr_1) = \max_u \{\min_{k \in K_u} \{mz_{ku}(kr_1) \mid \mu_{MU}(ug_n, mz_{ku}) > 0\}\}$$

Here $\min_{k \in K_u} \{mz_{ku}(kr_1) \mid \mu_{MU}(ug_n, mz_{ku}) > 0\}$ – the minimum value of the criterion kr_1 for mz_{ku}, neutralizing the threat ug_n level $ur_u \in UR$, $ug_n(kr_1)$ – the maximum value of the

neutralizing current threats and available security features. At each level of protection selected security functions with minimum cost, and to neutralize threats at all levels of system protection is considered the worst option is used – the security function with the maximum value.

B. Average rating (criterion kr_2)

1) Weighted average number of threats neutralized. Quantitative evaluation criteria for security features is going to be calculated by the formula:

$$kr_2 = \frac{1}{\left(1+\left(\frac{|UG_k| - sm^{mz_{ku}}}{a_2}\right)\right)^{b_2}},$$

where $UG_k = \{ug_n \mid \mu_{MU}(ug_n, mz_{ku}) > 0\}$ – many threats, neutralized security function mz_{ku}, $sm^{mz_{ku}} = \sum_{n=1}^{N} \mu_{MU}(ug_n, mz_{ku})$ – the sum of the scores of possibilities of neutralizing the threats security function a_2, b_2 – custom settings. As a parameter a_2 you must select the $\max_{ku}(|UG_k| - sm^{mz_{ku}})$ – the maximum difference between the number of threats and amount of estimated capabilities to neutralize threats security function mz_{ku} level u.

2) Weighted average number of protection features, neutralizing the current threat. Quantitative evaluation criteria for threats is going to be calculated by the formula:

$$ug_n(kr_2) = \min_u \{\max_{k \in K_u} \{mz_{ku}(kr_2) \mid \mu_{MU}(ug_n, mz_{ku}) > 0\}\}.$$

The levels of protection selected security functions with the maximum grade weighted average number of neutralized threats. To assess the neutralization of threats at all levels of protection considered the option of application security functions with a minimum weighted average rating number of neutralized threats.

C. Preventable risk (criterion kr_3)

1) The risk of vaccine-preventable security function. The risk from implementation of threats were previously identified as $rsk^{ug_n} = p^{ug_n} \times uch^{ug_n}$. Then $rsk_{mz_{ku}}^{\max} = \max_{n=1}^{N} rsk^{ug_n} \times (1 - \mu_{MU}(ug_n, mz_{ku}))$ - the maximum risk from the implementation of threats that were not neutralized by the security function mz_{ku} on the level of protection u, and the criterion value kr_3 for mz_{ku} you can define the following:

$$kr_3 = \frac{1}{\left(1+\left(\frac{rsk_{mz_{ku}}^{\max}}{a_3}\right)\right)^{b_3}},$$

where a_3, b_3 – custom settings. Option $a_3 = rsk_{mz_{ku}}^{\partial on}$ takes the value of permissible level of risk from the threat is credible.

Assume that the actual threat neutralized at least one security feature.

2) The risk from the threat is credible. The amount of risk from the implementation of the threats rate the following

$$ug_n(kr_3) = \min_u \{\max_{k \in K_u} \{mz_{ku}(kr_3) \mid \mu_{MU}(ug_n, mz_{ku}) > 0\}\}.$$

The levels of protection selected security function, which can prevent maximum damage from the threat is credible. In General, the levels of protection accepted the option of causing the minimum of damage from the threat is credible.

D. Power of attorney (criterion kr_4)

1) The level of proxy protection features. The level of proxy $kr_4 = sd_{mz_k}$ security function can be determined using the results of [6].

2) The level of proxy security function against the escape threats is calculated as

$$ug_n(kr_4) = \min_u \{\max_{k \in K_u} \{mz_{ku}(kr_4) \mid \mu_{MU}(ug_n, mz_{ku}) > 0\}\}.$$

For protection levels, a preference function of protection with a maximum rating of degree a power of attorney. In General, the levels of protection at the neutralization of threats are characterized by the use of the least-trusted security features.

E. Compatibility (criterion kr_5)

1) Compatibility security features. On a variety $mz_{ku} \in MZ$ we define the relation SV as follows: $\mu_{SV}(mz_\kappa, mz_j) \in [0,1]$ – degree of compatibility mz_k with mz_j. The opposite may be true: mz_j may not be compatible with mz_{iu}. Compatibility mz_k with other security features on the criterion kr_5 defined as follows:

$$kr_5 = \frac{1}{\left(\frac{1+(|SV_k| - sm_{mz_k}^{SV})}{a_5}\right)^{b_5}},$$

where $SV_k = \{mz_j \mid \mu_{SV}(mz_k, mz_j) > 0\}$ – many security functions, compatible with mz_k, $sm^{SV}_{mz_k} = \sum_{i=1}^{K} \mu_{SV}(mz_k, mz_i)$ – the sum of the degrees of compatibility mz_i with mz_k, a_5, b_5 – configurable.

2) Assessment of the degree of compatibility of the security functions in relation to neutralized threats:

$$ug_n(kr_5) = \min_u \{\max_{k \in K_u} \{mz_{ku}(kr_5) \mid \mu_{MU}(ug_n, mz_{ku}) > 0\}\}.$$

Levels of protection apply security function with the maximum grade the degree of compatibility. The structure of the information security system in the neutralization of threats are characterized by the least compatible of the levels of protection.

V. THE ALLOCATION OF SECURITY FUNCTIONS FOR NUMEROUS NEUTRALIZED THREATS

The allocation of security functions $mz_{ku} \in MZ$ to escape many threats to information security $ug_n \in UG$ associated with the choice of decision rules for such distributions.

A. The decision rule for the distribution

According to the approach [6] is required to determine the threshold of semantic preference in the allocation of security functions for neutralized threats to information security.

The General rule is that to choose the highest value pr, but less $\min_{i,j} \max_{mz} [1 - \min\{1, [(1-\mu_{\tilde{A}_i}(mz))^p + (1-\mu_{\tilde{A}_j}(mz))^p]^{\frac{1}{p}}\}]$.

Here, $\tilde{A}_1, \tilde{A}_2, ..., \tilde{A}_N$ the fuzzy sets representing the degree of neutralizing of threats $ug_n \in UG$, $n = \overline{1, N}$, security function mz_k.

The article applied is different from [9-12] and is known from the scientific literature alternative intersection operation

$$^{A}\mu_{\tilde{A} \cap \tilde{B}}(x) = 1 - \min\{1, [(1-\mu_{\tilde{A}}(x))^p + (1-\mu_{\ddot{B}}(x))^p]^{\frac{1}{p}}\}, \; p \geq 1$$

B. The source data

Identified a variety of protection features $mz_k \in MZ$, $k = \overline{1, K}$, current threats $ug_n \in UG$, $n = \overline{1, N}$, and the criteria of efficiency $kr_j \in KR$, $j = \overline{1, J}$, security features.

1) Evaluation of security functions. On the sets MZ and criteria KR we define the relation $M\tilde{R}$ – $\mu_{M\tilde{R}} : MZ \times KR \to [0,1]$. For all $mz_k \in MZ$ and all $kr_j \in KR$ $\mu_{M\tilde{R}}(mz_k, kr_j)$ – evaluation of security functions mz_k for private performance criterion kr_j.

Attitude will be presented in a matrix form:

$$M\tilde{R} = \| \mu_{M\tilde{R}}(mz_k, kr_j) \|, \; k = \overline{1, K}, \; j = \overline{1, J}.$$

2) Assessment of security threats. Next on the set criteria KR and current threats UG will form a relationship $K\tilde{G}$ – $\mu_{K\tilde{G}} : KR \times UG \to [0,1]$. For all $kr_j \in KR$ and all $ug_n \in UG$ $\mu_{K\tilde{G}}(kr_j, ug_n)$ – threat assessment ug_n according to the criterion kr_j determined by the necessity of neutralizing the threat ug_n protection feature mz_k.

In matrix form the relation takes the form

$$K\tilde{G} = \| \mu_{M\tilde{G}}(mz_j, kr_n) \|, \quad j = \overline{1, J}, \; n = \overline{1, N}.$$

3) Weighted cost of neutralizing the threat. On the basis of relationships $M\tilde{R}$ and $K\tilde{G}$ you can form a relationship $M\tilde{G}$ presented below:

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

The elements in the matrix we define as follows:

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

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

The amount $\sum_{kr} \mu_{M\tilde{R}}(mz, kr)$ is interpreted as a number of important criteria kr, characterizing the properties of mz_k, and $\mu_{\tilde{A}_n}(mz_k, ug_n)$ represents the weighted degree of neutralisation of actual threats ug_n security function mz_k.

4) The correctness of the implementation of security functions. Previously, when determining the value $\mu_{\tilde{A}_i}(mz_k)$ were not made assumptions regarding the correctness of the implementation of the security functions. Now the values of criteria of efficiency of the security functions included in the computed values $\mu_{\tilde{A}_i}(mz_k, ug_i)$.

According to the adopted approach is formed matrix W

$$\tilde{W} = \begin{bmatrix} \mu_{\tilde{A}_1}(mz_1, ug_1) \cap \mu_{\tilde{A}_2}(mz_1, ug_2), ..., \mu_{\tilde{A}_{N-1}}(mz_1, ug_{N-1}) \cap \mu_{\tilde{A}_N}(mz_1, ug_N) \\ \mu_{\tilde{A}_1}(mz_2, ug_1) \cap \mu_{\tilde{A}_2}(mz_2, ug_2), ..., \mu_{\tilde{A}_{N-1}}(mz_2, ug_{N-1}) \cap \mu_{\tilde{A}_N}(mz_2, ug_N) \\ ..... \\ \mu_{\tilde{A}_1}(mz_K, ug_1) \cap \mu_{\tilde{A}_2}(mz_K, ug_2), ..., \mu_{\tilde{A}_{N-1}}(mz_K, ug_{N-1}) \cap \mu_{\tilde{A}_N}(mz_K, ug_N) \end{bmatrix}$$

C. Semantic threshold preferences

Semantic threshold preference functions on the escape threats is determined from the condition

$$pr < \min_{i,j} \max_{mz} [1 - \min\{1, [(1 - \mu_{\tilde{A}_i}(mz))^p + (1 - \mu_{\tilde{A}_j}(mz))^p]^{\frac{1}{p}}\}], \; p \geq 1$$

Semantic preference threshold is used to select the functions of protection, the most effectively neutralizing the threat $ug_n \in UG$ to levels of protection in the structure of information security system as a whole.

$$M_{nu} = \{mz_{ku} \mid \mu_{\tilde{A}_n}(mz_{ku}, ug_n) \geq \min_{ij} \max_{mz_{ku}} \min[\mu_{\tilde{A}_i}(mz_{ku}, ug_i), \mu_{\tilde{A}_j}(mz_{ku}, ug_j)]$$

– many features of protection mz_{ku} , which can neutralize the threat ug_n on the level of protection $ur_u \in UR$; $M_n = \{mz_{ku} \mid \max_k \mu_{\tilde{A}_n}(mz_{ku}, ug_n)\}$, $u = \overline{1, U}$, $n = \overline{1, N}$. Here M_n – multiple protection features, effectively neutralizing ug_n most of the threat levels $ur_u \in UR$ of protection .

The proposed method of adaptation of the system of information security of automated systems to escape the threats used in the design, development and maintenance of security systems.

VI. CONCLUSIONS

The optimality of the feature sets of the protection levels of the information security system for automated systems not yet proves the optimality of these sets to neutralize threats to information security.

The proposed method of distribution of the security features on the escape threats to information security of automated systems, allowing to structure the information security system by distributing the functions of protection for many neutralized threats in information security protection levels.

Justified a hypothesis about the identity of the system evaluation criteria security threats and neutralizing their protection features.

Defined semantic threshold of preference in the allocation of security functions for neutralized threats to information security, allowing you to select

the security function, effectively neutralizing most of the threat to levels of protection in the structure of information security system as a whole.

The proposed method of distribution of the security features on the escape threats used in the design, development and maintenance of systems for the protection of automated systems.

REFERENCES

[1] Aslan M., Matrawy A. Could network view inconsistency affect virtualized network security functions? In Proc. Of the 2017 IEEE Conference on Communications and Network Security (CNS), IEEE, 2017, pp. 510 – 512. DOI: 10.1109/CNS.2017.8228698

[2] Hyun S., Kim J. Kim H., Jeong J., Hares S., Dunbar L., Farrel A. Interface to Network Security Functions for Cloud-Based Security Services. IEEE Communications Magazine, 2018, vol 56, N 1, pp. 171-178 DOI: 10.1109/MCOM.2018.1700662

[3] Kim S.-H., Eom J.-H., Chung T.-M. A study on optimization of security function for reducing vulnerabilities in SCADA. In Proceedings of the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). 2012, pp. 65-69. DOI: 10.1109/CyberSec.2012.6246099.

[4] Zakharenkov A. I., Butusov, I. V., Romanov A. A. The degree of confidence of software and hardware as a measure of quality import substitution. Voprosy kiberbezopasnosti *[Cybersecurity issues]*. 2017. N 4(22), pp. 2–9. DOI: 10.21681/2311-3456-2017-4-2-9.

[5] Barabanov A., Markov A. Modern Trends in The Regulatory Framework of the Information Security Compliance Assessment in Russia Based on Common Criteria. In Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN '15. ACM New York, NY, USA, 2015, pp. 30-33. DOI: 10.1145/2799979.2799980.

[6] Butusov I.V., Nasekin P.A., Romanov A.A. Theoretical and semantic aspects of the organization of a comprehensive system of protection of information systems. Voprosy kiberbezopasnosti *[Cybersecurity issues]*. 2016. N 1(14), pp. 9-16. DOI: 10.21681/2311-3456-2016-1-9-16.

[7] Barabanov A., Markov A., Fadin A., Tsirlov V., Shakhalov I. Synthesis of Secure Software Development Controls. In Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN '15. ACM New York, NY, USA, 2015, pp. 93-97 DOI: 10.1145/2799979.2799998.

[8] Fuzzy sets and theory of possibilities. The latest advances. By ed. Yager R.R. Pergamon, 1982, 633 p.

[9] Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K. Analysis of computer security incidents using fuzzy logic. In Proceedings of the 20th IEEE International Conference on Soft Computing and Measurements (24-26 May 2017, St. Petersburg, Russia). SCM 2017, 2017, pp. 369 - 371. DOI: 10.1109/SCM.2017.7970587.

[10] Bykov A. Yu., Gurov A. V., Problem of choice of means of protection of information from attacks in automated systems with fuzzy parameters the objective function. Engineering journal: science and innovations. Electronic scientific and technical periodical. 2012. N 1(1). DOI: 10.18698/2308-6033-2012-1-86

[11] Andreev A. G., Kazakov G. V., Kuranov V. V. Method of assessing the strength of security functions protection of automated control system of the spacecraft mission. Engineering journal: science and innovation. Electronic scientific and technical edition. 2017. N 7(67). DOI: 10.18698/2308-6033-2017-7-1634

[12] Tamjidyamcholo A., Yamchello H.T.,Bin M.S., Gholipour R. Application of fuzzy set theory to evaluate the rate of aggregative risk in information security. In Proc. of the 2013 International Conference on Research and Innovation in Information Systems (ICRIIS), IEEE, pp. 410 – 415. DOI: 10.1109/ICRIIS.2013.6716745.