Formation of multilevel system to counteract computer attacks

V.A. Minaev[1], A.V. Koryachko[2], K.M. Bondar[3]
m1va@yandex.ru|akor89@yandex.ru|bondar_km@mail.ru.
[1]Bauman Moscow state technical university, Moscow, Russia;
[2]Ryazan state radio engineering university named after V.F. Utkin, Ryazan, Russia;
[3]Far Eastern Law Institute of the Ministry of Internal Affairs of Russia, Khabarovsk, Russia

The main trend relating to state structures and large corporations is to build Information Security Monitoring Centers the key elements of which being SIEM-systems and SOC-Centers. Speaking about SOC-Centers the task of human resources optimal allocation among information security incident reporting lines taking into consideration staff competency and line capacity seems to be urgent. This task is solved in the article given. In general, the formulation of the task presented means the functioning of SOC-Center as a new mathematical model making use of "input – resources – output" terms. The target function of SOC-Center is built in an assumption of stationarity and independency of service reporting lines as a sum of their target functions. The main idea of human resources management in this case is the aspiration to achieve maximum significance of SOC-Center system aim, i.e. its general target function when organizing the fight with computer attacks. The problem was solved by Lagrange multiplier method. The expressions for optimal allocation of human resources on SOC-center service lines leading to maximum processing of message flow related to computer attacks have been received. The conclusion about this model being useful for transferring from stationary flows to their dynamic changes in SOC-Center resource provision including new different critical situations in computer system has been made.

***Key words**: SOC-center, modeling, computer attack, human resources, optimal allocation.*

1. Introduction

Modern state structures being referred as critical ones as well as geographically distributed intersectoral and large industrial corporations form complex Information Security Monitoring Centers (ISMC) [1-3]. The structural elements of these Centers are represented as the devices to collect incidents arising in external and internal sources (user devices, network devices, different systems of information defense, web-services, etc.) Primary monitoring segment of ISMC is SIEM – systems. SIEM (Security Information and Event Management) technology presupposes automated real-time analysis of security events in network devices and applications. The next segment of monitoring, processing and reaction to information security incidents in ISMC is SOC – center (Security Operation Center) that receives notifications about threats from SIEM – system where operators being qualified employees in the sphere of information security make decisions concerning the reports about threats. Mathematical modeling of SIEM – system and SOC – center functioning processes is of utmost importance to improve the control of information security in organizations [2, 3]. This fact is caused by the necessity to create scientific apparatus allowing to efficiently solve the problems connected with optimal ISMC resources control, with evaluation, analysis and forecasting of computer attacks, etc. The article given considers the model to optimize SOC-center human resources allocation on information security incident reporting lines taking into consideration staff competence and line capacity.

2. Materials and methods

The formulation of management task is as follows.

Let there be a certain multitude of problems to respond on information security incidents, for them to be solved SOC-center needs to have a certain amount of human resources. Human resources need to be optimally allocated among service levels (decision making levels) taking into account a number of limitations.

ISMC material and technical resources can be considered in this case as the tools increasing the realization opportunities of the staff that play the leading role in the process of problem solution. Particularly, different level of logistics in corresponding mathematical models is seen in different parameters reflecting the efficiency in staff activity of SOC-center that provides the services on computer attacks incident reporting lines.

Further let us designate the flow of input reports about computer incidents as input vector $\vec{X}$, the result of report processing in SOC-center – as output vector $\vec{V}$, $\vec{R}$ designates the vector of human resources being competent in decision making referring to computer incidents. General form in the dependence of output variables vector from input variables vector as well as human resources vector is as follows:

$$\vec{V} = \bar{V}\ (\vec{R},\vec{X})\ , \qquad (1)$$

meeting the condition: $\sum_{i=1}^{i=I} R_i = R_0$, where I – is general number of SOC-center reporting lines; R_i – the staff that provides services for i-th line, i = 1,2,..I; R_0 – general staff providing services for all lines.

By analogy with production processes described in the applications of the theory of active systems [4-6] we shall name the functional connection between acceptable level of resource costs and input vector, on the one hand, and output variable extreme values (minimum and maximum) corresponding to them – on the other hand, as production or target function:

$$\bar{V}_{Extr} = \bar{V}\ (\bar{R},\bar{X})\ , \qquad (2)$$

when $\sum_{i=1}^{I} R_i = R_0$.

Two main approaches to build target functions – statistic and optimization – can be mentioned [7, 8]. The first one is based on statistics dependency recovery. The second approach is based on generalizing the solutions of tasks analogous to the ones in other areas as well as theoretical speculations and assumptions.

The article presented follows the second approach where mathematical model "costs – results" is given by introducing target function of the following type:

$$\varphi_i = \varphi_i\ (F_i, R_i, \bar{\mu}) \qquad (3)$$

where F_i – the number of attack incidents in i-th line, R_i – number of employees servicing i-th line, $\overline{\mu}$ – target function parameters vector in i-th line.

We shall assume that function (3) monotonically increases in the area $0 < R_i < \infty$, i.e., the higher SOC-Center staffing is, the higher the value of target function:

$$\varphi_i = \varphi_i\left(F_i, \infty, \overline{\mu}_i\right) = A_i = const, \qquad (4)$$

with the function being limited in the upper part (Fig. 1). These conditions are satisfied by the function of the type:

$$\varphi_i = A_i \cdot (1 - \exp(-\beta_i * h_i)), \qquad (5)$$

where β_i – is the coefficient reflecting competency and professionalism of the staff in i-th SOC line that process computer attack incidents; $h_i = F_i/R_i$ – load on the staff in i-th line.

The choice of the function being type (5) is offered in works [9, 10] to describe the efficiency of fire service activity depending on the load on firefighters. In our opinion, when necessary statistical data to build target function in relation to SOC-Center activity are absent, the choice of well-adapted, logic and interpreted dependence is appropriate and justified (5).

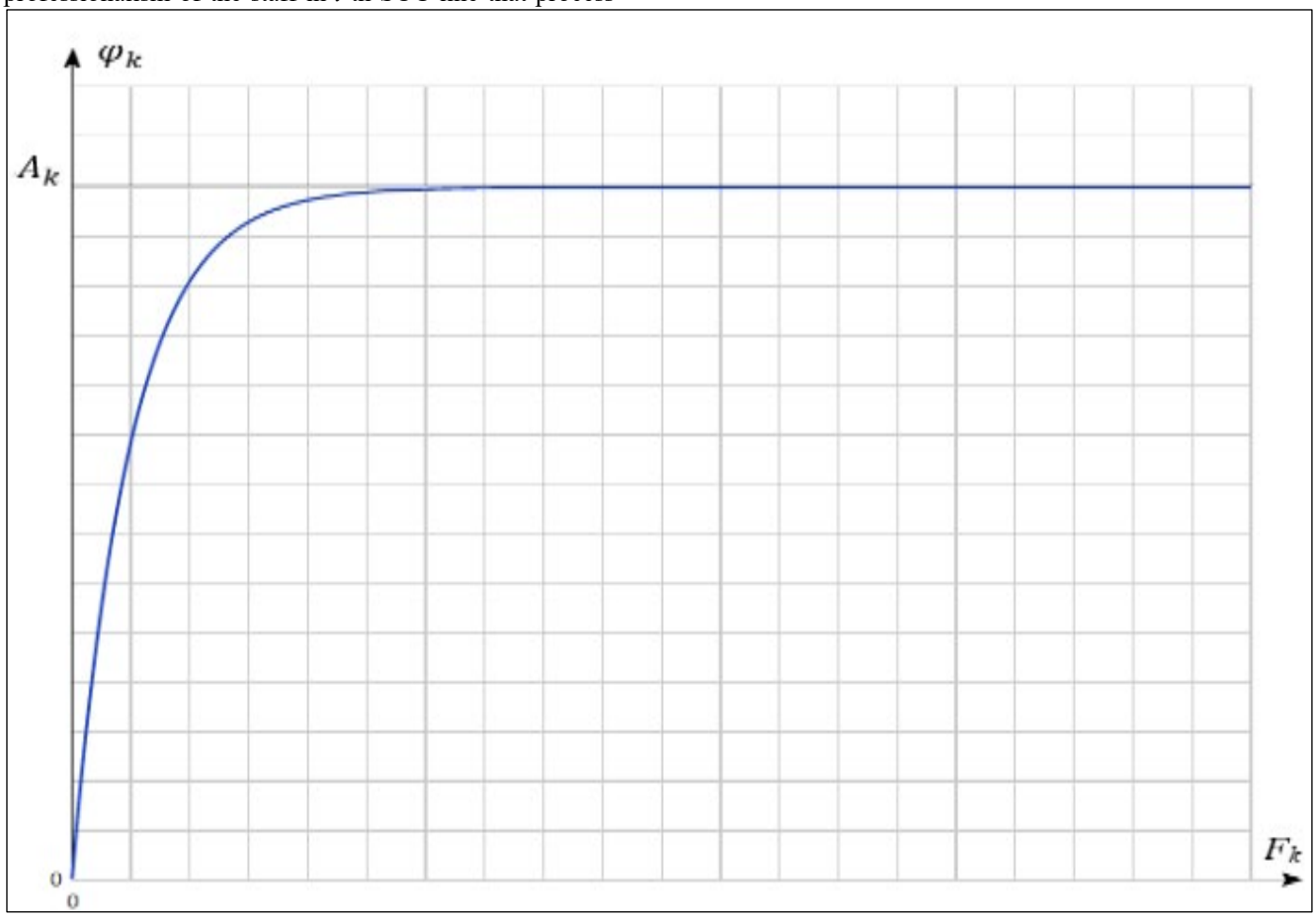

Fig. 1. Type of target function (5)

Based on the results received in works [9, 10], target function $\Phi_ц$ of the whole SOC – center can be determined as the sum of all target functions for each line:

$$\Phi_ц = \sum_{i=1}^{i=I} \varphi_i \qquad (6)$$

An important idea to manage human resources in this case is the aspiration for SOC – center to achieve a certain optimal value of its system aim, i.e. a general target function while determining the target functions of active elements (SOC – center lines) by choosing such allocation of human resources which will promote upgrading forms and methods of working activity as well as maximum staff involvement when organizing the fight with computer attacks.

The task to allocate human resources in the dependence given (3) and known parameters $\bar{\mu}_i$ is set as the following optimization task:

$$\Phi_{max} = \max_{R}[\sum_{i=1}^{i=I} \varphi_i\ (F_i, R_i, \bar{\mu})], \qquad (7)$$

in case when human resources being at SOC – Center disposal is limited: $\sum_{i=1}^{i=I} R_i = R_0$.

Such principle of human resources allocation is called *optimal allocation principle*.

Further we shall assume that the allocation of computer attack incident flow among three reporting lines of SOC – Center (i.e. $I = 3$) is implemented according to the diagram presented in Fig. 2.

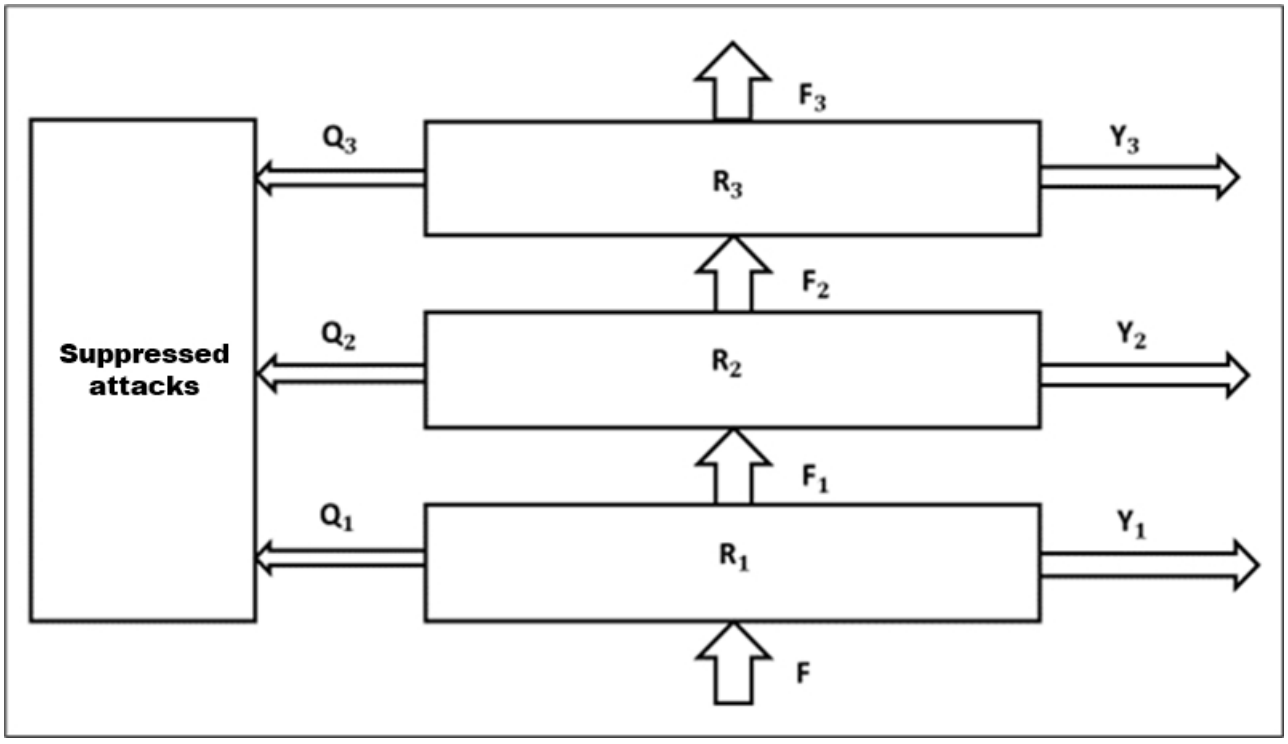

Fig.2. Diagram of allocating input and processed reports about computer attacks in SOC – center

It is worth mentioning that the results received in the work are easily generalized to other options of SOC – Center organization bearing in mind the number of reporting lines.

The diagram shows that all reports about computer attacks entering the first and the second SOC – Center lines are subdivided into three categories regarding to which the staff makes one of three decisions: *first* – the ones representing no threat for computer system $(Y_i); i = 1,2,3$; *second* – repulsed attacks $(Q_i); i = 1,2,3$; *third* - the ones transferred to a more competent and higher level of decision making $(F_i); i = 1,2,3$. The third line, the one where the most competent employees work is supposed to transfer the reports with no decisions being made to a special database in the form of F_3 flow for further in-depth examination.

We shall assume that in a certain period of time a stationary mode of processing computer attack reports is seen. Then for three SOC – Center lines the following nine equations are satisfied:

$$\begin{gathered} F = Y_1 + F_1 + Q_1 \\ Y_1 = A_{Y_1} \cdot [1 - \exp(-\beta_{Y_1} \cdot \frac{F}{R_1})] \\ Q_1 = A_{Q_1} \cdot [1 - \exp(-\beta_{Q_1} \cdot \frac{F}{R_1})] \\ F_1 = Y_2 + F_2 + Q_2 \\ Y_2 = A_{Y_2} \cdot [1 - \exp(-\beta_{Y_2} \cdot \frac{F_1}{R_2})] \\ Q_2 = A_{Q_2} \cdot [1 - \exp(-\beta_{Q_2} \cdot \frac{F_1}{R_2})] \\ F_2 = Y_3 + Q_3 + F_3 \\ Y_3 = A_{Y_3} \cdot [1 - \exp(-\beta_{Y_3} \cdot \frac{F_2}{R_3})] \\ Q_3 = A_{Q_3} \cdot [1 - \exp(-\beta_{Q_3} \cdot \frac{F_2}{R_3})], \end{gathered} \tag{8}$$

where A_{Y1}, A_{Q1}; A_{Y2}, A_{Q2}; A_{Y3}, A_{Q3} - constants, characterizing flow asymptotes that reflect the number of reports received by line operators having no threats to computer systems and the number of repulsed attacks correspondingly. In their turn, $\beta_{Y_1}, \beta_{Q_1}; \beta_{Y_2}, \beta_{Q_2}$; β_{Y_3}, β_{Q_3} – are the coefficients that reflect competency and professionalism of employees working on 1st, 2nd, and 3rd SOC lines to process computer attack reports, correspondingly. Here, the higher the service line, the higher the competence.

The following notations for loads in *i*-th line of SOC – center are introduced:

$$h_1 = \frac{F}{R_1}; h_2 = \frac{F_1}{R_2}; h_3 = \frac{F_2}{R_3} \tag{9}$$

To simplify further calculations we shall expand exponential expressions from (8) in Maclaurin series restricting ourselves to the first two terms for simplicity:

$$\begin{gathered} F = Y_1 + F_1 + Q_1 \\ Y_1 = A_{Y_1} \cdot [1 - 1 + \beta_{Y_1} \cdot h_1] \\ Q_1 = A_{Q_1} \cdot [1 - 1 + \beta_{Q_1} \cdot h_1] \\ F_1 = Y_2 + F_2 + Q_2 \\ Y_2 = A_{Y_2} \cdot [1 - 1 + \beta_{Y_2} \cdot h_2] \\ Q_2 = A_{Q_2} \cdot [1 - 1 + \beta_{Q_2} \cdot h_2] \\ F_2 = Y_3 + F_3 + Q_3 \\ Y_3 = A_{Y_3} \cdot [1 - 1 + \beta_{Y_3} \cdot h_3] \\ Q_3 = A_{Q_3} \cdot [1 - 1 + \beta_{Q_3} \cdot h_3] \end{gathered} \tag{10}$$

Simplifying (10), we get:

$$\begin{gathered} F = Y_1 + F_1 + Q_1 \\ Y_1 = A_{Y_1} \cdot \beta_{Y_1} \cdot h_1 \\ Q_1 = A_{Q_1} \cdot \beta_{Q_1} \cdot h_1 \\ F_1 = Y_2 + F_2 + Q_2 \\ Y_2 = A_{Y_2} \cdot \beta_{Y_2} \cdot h_2 \\ Q_2 = A_{Q_2} \cdot \beta_{Q_2} \cdot h_2 \\ F_2 = Y_3 + Q_3 + F_3 \\ Y_3 = A_{Y_3} \cdot \beta_{Y_3} \cdot h_3 \\ Q_3 = A_{Q_3} \cdot \beta_{Q_3} \cdot h_3 \end{gathered} \tag{11}$$

Next we introduce the notation:

$$\alpha = A_{Y_1} \cdot \beta_{Y_1} + A_{Q_1} \cdot \beta_{Q_1} \quad (12)$$

Then

$$Y_1 + Q_1 = \alpha \cdot h_1 \quad (13)$$

By analogy

$$Y_2 + Q_2 = \gamma \cdot h_2, \quad (14)$$

where

$$\gamma = A_{Y_2} \cdot \beta_{Y_2} + A_{Q_2} \cdot \beta_{Q_2}, \quad (15)$$

As well as

$$Y_3 + Q_3 = \delta \cdot h_3, \quad (16)$$

where

$$\delta = A_{Y_3} \cdot \beta_{Y_3} + A_{Q_3} \cdot \beta_{Q_3} \quad (17)$$

3. Solving the task of human resources optimal distribution

Balance ratios in (10) easily show that

$$F - F_3 = \sum_{i=1}^{i=3}(Y_i + Q_i) = \alpha \cdot h_1 + \gamma \cdot h_2 + \delta \cdot h_3 \quad (18)$$

Then the task of optimal human resources allocation among SOC – Center incident reporting lines is set as:

$$\Phi_{u\,max} = \max_{R_i}[\alpha \cdot h_1 + \gamma \cdot h_2 + \delta \cdot h_3], \quad (19)$$

limiting the number of human resources:

$$\sum_{i=1}^{i=3} R_i = R_0. \quad (20)$$

The task (19) - (20) will be solved by the method of Lagrange multipliers.

Lagrange function is written as:

$$L(\Phi_u, \lambda) = \alpha \cdot h_1 + \gamma \cdot h_2 + \delta \cdot h_3 - \lambda \cdot (\sum_{i=1}^{i=3} R_i - R_0), \quad (21)$$

where λ – is Lagrange multiplier.

We shall substitute (21) with expressions from (9) for $h_i; i = 1,2,3.$

$$L(\Phi_u, \lambda) = \alpha \cdot \frac{F}{R_1} + \gamma \cdot \frac{F_1}{R_2} + \delta \cdot \frac{F_2}{R_3} - \lambda \cdot (\sum_{i=1}^{i=3} R_i - R_0). \quad (22)$$

We shall believe that in case of stationary mode $F, F_1\, u\, F_2$ – are constant, then conditional extremum of expression (22) is found from ratios:

$$\frac{\partial L(\bar{R},\lambda)}{\partial R_i} = \frac{\partial L(\bar{R},\lambda)}{\partial \lambda} = 0;\ i = 1, 2, 3. \quad (23)$$

Having done differentiation we come to the system of equations:

$$\begin{aligned} \frac{\partial L(\bar{R},\lambda)}{\partial R_1} &= -\alpha \cdot \frac{F}{R_1^2} - \lambda = 0 \\ \frac{\partial L(\bar{R},\lambda)}{\partial R_2} &= -\gamma \cdot \frac{F_1}{R_2^2} - \lambda = 0 \\ \frac{\partial L(\bar{R},\lambda)}{\partial R_3} &= -\delta \cdot \frac{F_2}{R_3^2} - \lambda = 0 \\ \frac{\partial L(\bar{R},\lambda)}{\partial \lambda} &= \sum_{i=1}^{i=3} R_i - R = 0 \end{aligned} \quad (24)$$

From system (24) we obtain:

$$\begin{aligned} \alpha \cdot \frac{F}{R_1^2} = \gamma \cdot \frac{F_1}{R_2^2} = \delta \cdot \frac{F_2}{R_3^2} \\ \sum_{i=1}^{i=3} R_i = R \end{aligned} \quad (25)$$

Equations (25) can easily give expressions for such human resources allocation on SOC – Center reporting lines that lead to the maximum processing of computer attack incident report flow on computing system of the organization. Namely:

$$\begin{aligned} R_1 &= R_0 \cdot \frac{\sqrt{\alpha \cdot F}}{\sqrt{\alpha \cdot F} + \sqrt{\gamma \cdot F_1} + \sqrt{\delta \cdot F_2}}, \\ R_2 &= R_0 \cdot \frac{\sqrt{\gamma \cdot F_1}}{\sqrt{\alpha \cdot F} + \sqrt{\gamma \cdot F_1} + \sqrt{\delta \cdot F_2}} \\ R_3 &= R_0 \cdot \frac{\sqrt{\delta \cdot F_1}}{\sqrt{\alpha \cdot F} + \sqrt{\gamma \cdot F_1} + \sqrt{\delta \cdot F_2}}. \end{aligned} \quad (26)$$

Besides, making use of ratios (11) we easily show that

$$\begin{aligned} F_1 &= F \cdot \left(1 - \frac{\alpha}{R_1}\right), \\ F_2 &= F \cdot \left(1 - \frac{\alpha}{R_1}\right) \cdot \left(1 - \frac{\gamma}{R_2}\right), \\ F_3 &= F \cdot \left(1 - \frac{\alpha}{R_1}\right) \cdot \left(1 - \frac{\gamma}{R_2}\right) \cdot \left(1 - \frac{\delta}{R_3}\right). \end{aligned} \quad (27)$$

From (27) we see that

$$0 < \alpha < R_1;\ 0 < \gamma < R_2;\ 0 < \delta < R_3. \quad (28)$$

Besides, (28) leads to inequality fairness:

$$F_3 < F_2 < F_1 < F \quad (29)$$

Taking into consideration the dependences of flows F_i from human resources allocation on reporting lines $R_i; i = 1,2,3,$ a recursive algorithm to find optimal solution has been developed. To justify the values of model parameters, initial conditions and asymptotic values the results received in works [11-15] have been applied in the system to counteract computer attacks.

4. Results

The model of SCO – center operation being developed in the article under consideration have allowed us to describe the system of multilevel computer attack reporting service taking into account competency of employees and capacity of the channels that react to information security incidents. Formalization of the processes that react to reports about incidents in the model justified and implemented by the authors allows studying:

- efficiency of different allocations in human resources being at SOC – Center disposal to fight with computer attacks, viz., to find the allocation with maximum result in the course of processing the reports about threats to computing resources and cutting off real threats from them;
- influence of such factors as competency and professionalism of SOC – Center employees in different service reporting lines on suppression of computer attacks;
- errors of first and second order in each reporting line;
- possibilities to justify and transfer from stationary flows in the model to their dynamic changes including different critical situations of SOC – Center resource provision.

Acknowledgements

The work has been implemented and published with the RFBR support, grant 19-07-00445.

References

[1] Minaev V.A., Bondar K.M., Vaits Ye.V., Belyakov I.A. Discrete and event modelling of monitoring and management processes of information security //

Vestnik of Russian New University. 2019. № 3. – Pp. 32-39.
[2] Shaburov A.S., Borisov V.I. Developing the model of corporate network information protection based on the implementation of SIEM-System // Vestnik of PSTU. 2016. № 19. – Pp.111-124.
[3] Zimmerman C. Ten Strategies of a World-Class Cybersecurity Operations Center. The MITRE Corporation, US. 2014. – 334 c.
[4] Novikov D.A., Petrakov S.N. The course of active systems theory. M.: SINTEG, 1999. – 104 p.
[5] Burkov V.N. Foundations of mathematical theory of active systems. – M.: Nauka, 1977. – 255 p.
[6] Burkov V.N., Kondratiev V.V. Mechanisms of organization system functioning. – M.: Nauka, 1981. – 333 p.
[7] Minaev V.A. Human Resources of the Internal Affairs Bodies: Modern Management Approaches: Monograph. M.: Academy of the Ministry of Internal Affairs of the USSR, 1991. – 163 p.
[8] Burkov V.N., Burkova I.V. Network programming method in target programs management // Automation and telemechanics. 2014. № 3. – Pp. 73–86.
[9] Bessonov V.A. Problems of production functions formation in Russian transitional economy. M.: Institute for the economy in transition, 2002. – 89 p.
[10] V.A. Minaev, N.G. Topolskij, T.A. Kjeu. Criteria management of territorial allocation of the fire service staff resources in Vietnam // Vestnik of Russian New University. Series: Complex systems: models, analysis and control. 2019. № 2. – Pp. 94-103.
[11] V.A. Minaev, N.G. Topolskij, T.A. Kjeu. Efficiency of territorial allocation of the fire service staff resources in Vietnam // Technologies of technosphere security. 2019. № 2. – Pp. 63 – 71.
[12] Klimov S.M., Sychyov M.P., Astrakhov A.V. Counteraction to computer attacks. Methodical bases: E-learning edition. M.: Publishing House of MSTU named after N.E. Bauman, 2013. – 108 p.
[13] ShaburovA.S., Mironova A.A. The detection of computer attacks based on the functional approach // Vestnik of Perm university. Series: Mathematics. Mechanics. Informatics. 2015. Issue 4 (31). – Pp. 110-115.
[14] Klimov S.M., Polovnikov A.Yu. Method to detect computer attacks on critically important information systems // Issues of information security. 2016. № 1 (112). – Pp. 48-55.
[15] Shlyapkin A.V. Methods and means to counteract attacks on computer networks // Information systems and technologies: control and security. 2014. № 3. – Pp. 325-338.
[16] Drobotun Ye.B. Theoretical foundations of building security systems from computer attacks on automated control systems: Monograph. – Saint Petersburg: High technologies, 2017. – 120 p.

About the authors

Minaev Vladimir A., Doctor in technical sciences, PhD, full professor, Bauman Moscow state technical university. E-mail: m1va@yandex.ru.

Koryachko Aleksei V., PhD (in technical sciences), associate professor, deputy rector, Ryazan state radio engineering university named after V.F. Utkin. E-mail: akor89@yandex.ru.

Bondar Konstantin M., PhD (in technical sciences), associate professor, Far Eastern Law Institute of the Ministry of Internal Affairs of Russia. E-mail: bondar_km@mail.ru.