Klimov S.M., Kotyashev N.N.

METHOD OF RISK MANAGEMENT FOR AUTOMATED SYSTEMS UNDER CONDITIONS OF CYBER ATTACKS

The paper considers a method for managing risks of automated systems under conditions of cyber attacks based on dynamic control and risk minimization of information resource violations. The method offers analytical expressions for target functionality and tolerances of risk factors enabling to make reasonable decisions on risk management of automated systems.

Keywords: *automated system, cyber attack, risk management.*

A topical issue of information security is justification of risk management requirements for application of automated systems (AS) in real time mode under conditions of cyber attacks.

By AS, we shall mean critical parts of automated systems that operate in modes near to real time, and with their parameters exceeding specified limits (time of collection, processing and transmission of information and issue of control actions), it leads to operation stability violation.

In this paper, we shall consider risk management for designed automated systems, whose state dynamically changes over time under conditions of cyber attacks.

The essence of AS risk management method is to minimize risks of the form R = PY → min, where P is the probability of the event that an intruder realizes a cyber attack within the time of detection; Y is the mathematical expectation of damage due to the impact of a cyber attack. Let there be an achieved risk level $R_0=P_0*Y_0$. Then the risk management consists in purposefully changing risk factors to the level that allows AS to realize its functionality according to the two possible criteria: reducing a risk to the desired values or minimizing a risk under existing limits of information resources.

The problem of AS risk management is solved in linear and nonlinear formulations. The studies [1, 2] have considered examples of risk management in linear formulation at low limits of risk factors that are reduced to a linear programming problem in normalized space of functional cost and limitations

$$\overline{S}\left(\overline{P},\overline{Y}\right)=\left(1-a\right)\cdot\overline{P}+\left(1-b\right)\cdot\overline{Y} \tag{1}$$

where $\overline{X}=\left(X-X_0\right)/X_0$; $\overline{X}_1\le\overline{X}\le\overline{X}_2,\ a,b$ are coefficients of costs for reducing risk factors.

Additive representation of the functional is obtained by writing and revealing the multiplicative form of the type (P0+dP)(Y0+dY) along with discarding the terms of the second order of smallness and adding (with the opposite sign) cost managerial constituents a(P-P_0)Y0 and b(Y-Y_0)P_0.

Due to the fact that the normalization operator does not change the position of an extreme point, this problem is also solvable for non-normalized risk factors, which simplifies the problem

$$S(P,Y)=(1-a)\cdot P+(1-b)\cdot Y \text{ , where } X_1 \le X \le X_2 .$$

Proof of such a substitution is done by verification of equality of partial derivatives of the functionals as per risk factors of AS operation stability under conditions of cyber attacks not only for linear functionals but also for arbitrary functionals as well as mutual reversibility of limitations. This statement follows from the propositions of the sensitivity theory that define relations between a functional and risk factors.

Risk management of AS under conditions of probabilistic uncertainty in specifying risk factors and their small variations using the sensitivity functions of the first order [3] is carried out as follows.

Let the risk of ensuring AS sustainability under cyber attacks is described by the expression

$$R=Y\cdot P$$

where Y and R are mean values for the probability of cyber attack realization and damage.

Write the expansion of a risk function in a Taylor series while retaining only linear terms in it

$$R\left(P,Y\right)=R_0\left(P_0,Y_0\right)+\left(1-\frac{dR}{dP}\right)\cdot dP+\left(1-\frac{dR}{dY}\right)\cdot dY .$$

Let also their initial values R_0 and Y_0 and hence the initial level of risk $R_0 = P_0*Y_0$ be set.

The corresponding functions of sensitivity as for parameters of risk will be

$$FZp=\left.\frac{\partial R}{P}\right|_{R_0}=\left.\frac{\partial(P\cdot Y)}{P}\right|_{R_0}=Y_0$$

And

$$FZp=\left.\frac{\partial R}{Y}\right|_{R_0}=\left.\frac{\partial(P\cdot Y)}{Y}\right|_{R_0}=P_0 .$$

The level of probabilistic uncertainty of individual risk factors in case of the normal error distribution of their specification will be respectively

$$\delta P=\chi_q\cdot\sigma_p$$

$$\delta Y=\chi_q\cdot\sigma_y$$

where χ_q and χ_y as well as σ_q and σ_y are corresponding quantiles and mean square deviations of the error distribution for these factors.

Then, the influence functions for the risk function of the above uncertainties will be

$$FWp=FZp\cdot\delta P$$

and

$$FWy = FZy \cdot \delta Y$$

Depending on the functional features of AS, they can be summed up arithmetically (the worst case) or geometrically

$$FW1 = FZp \cdot dP + FZy \cdot dY \,,$$

$$FW2 = \sqrt{(FZp \cdot dP)^2 + (FZy \cdot dY)^2} \,.$$

In general, the guaranteed risk will be

$$R_{\Gamma} = R_0 + FW.$$

So, for example, for P_0 = 0.5 and Y_0 = 20, therefore, R_0 = 10, FZp = 20, FZy = 0.5, the mean square deviation σ_p=0.1 and σ_y=1 as well as for uncertainty with the confidence of 0.993, the guaranteed level of risk for the worst case will be equal only to Rг=16.75.

The procedure error of linearity is found by the following expression

$$dR_{\text{г}} = R_{\text{г}} - P_{\text{г}} \cdot Y_{\text{г}} = P_0 \cdot Y_0 - (P_0 - \delta P) \cdot (Y_0 - \delta Y)$$

and will make up albeit quite a permissible value, 0.729, but it can change the management direction as per expression (1).

To compensate this total uncertainty in specifying only a single risk factor, such as management, it will require the introduction of the following managements

$$dPu = \frac{-1}{FZp} \cdot FW$$

and

$$dYu = \frac{-1}{FZy} \cdot FW \,.$$

In both cases, we will have a new guaranteed risk equal to the initial mean value

$$R_{\text{г}}^{\text{н}} = P_{\text{г}} \cdot Y_{\text{г}} = (P_0 - \delta P) \cdot Y_0 + FW = P_0 \cdot (Y_0 - \delta) + FW = R_0.$$

AS construction with minimal risk of operation stability violation through the use of sensitivity functions when there is a need to reduce a risk level to the desired value Rtr, is carried out as follows.

Let us set up a system of algebraic equations taking into account the equality of contributions of risk factors in the risk function of complex automated systems

$$FZ_p \cdot (P - P_0) = FZ_y \cdot (Y - Y_0)$$

and specified limits of the risk function value $P \cdot Y = Rtr$

$$\begin{cases} FZ_p \cdot (P - P_0) = FZ_y \cdot (Y - Y_0), \\ P \cdot Y = Rtr. \end{cases}$$

In view of $Ytr(Rtr) = Rtr / Ptr$, we shall reduce the first equation to the form

$$FZ_p \cdot (Ptr - P_0) - (FZ_y \cdot (\frac{Rtr}{Ptr} - Y_0)) = 0.$$

The root of this equation is the required value of Ptr (it is found using the computer mathematics means of MathCad «root») from the limit of the risk function value

$$Ytr(Rtr) = \frac{Rtr}{Ptr(Rtr)}.$$

Let Rtr = 1. Elementary calculations yield

Ptr(Rtr)=0.158 and Ytr(Rtr)=6.35.

Provided that $Ptr(Rtr) \cdot Ytr(Rtr) = 1$.

The values of risk factors are sensitive to their initial levels and to the level of requirements for the risk function (Fig. 1).

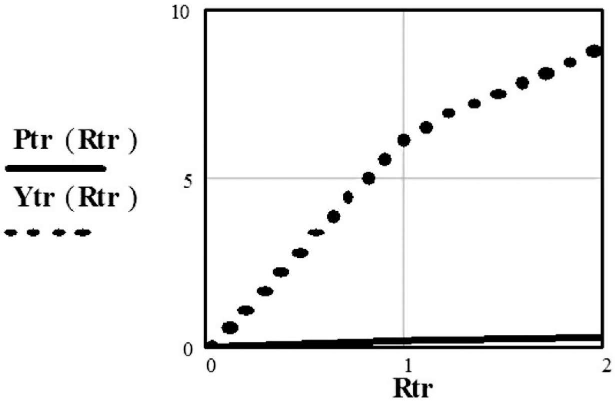

Fig. 1. Dependence of risk factors on the required levels of risk

It is quite important to have some analytical solution for defining values of the considered risks using sensitivity functions and costs under limits of a risk uncertainty level. Suppose it is required to reduce the guaranteed risk level of providing operation stability of AS.

$$R_z = P_0 \cdot Y_0 + FZ_p \cdot dP + FZ_y \cdot dY.$$

Let us reduce the current level of uncertainty in the most economical way to some predetermined level Rtr. First, we shall minimize the value of the functional of the following form

$$C_s = C_p \cdot (P_0 / dP)^{\nu} + C_y \cdot (Y_0 / dY)^{\nu}$$

where C_p and C_y are cost coefficients, v is the coefficient that provides the best approximation option. We also define the level of uncertainty of the following form

$$FZ_p \cdot dP + FZ_y \cdot dY = eps.$$

The problem is reduced to finding the unconditional extremum using Lagrange's principle. We write the Lagrangian of the form

$$FL(dP, dY, \lambda) = Cp \cdot (P0 / dP)^{v} + Cy \cdot (Y0 / dY)^{v} + \\ + \lambda \cdot \left[(FZp \cdot dP + FZy \cdot dY) - eps \right]$$

There is an analytical solution

$$dP = \frac{eps \cdot \left[Cp \cdot \left(P0^{v} / dP \right) \right]^{\frac{1}{1+v}}}{FZp \cdot \left[Cp \cdot \left(P0^{v} / dP \right) \right]^{\frac{1}{1+v}} + FZy \cdot \left[Cy \cdot \left(Y0^{v} / dY \right) \right]^{\frac{1}{1+v}}}$$

$$dY = \frac{eps \cdot \left[Cy \cdot \left(Y0^{v} / dY \right) \right]^{\frac{1}{1+v}}}{FZp \cdot \left[Cp \cdot \left(P0^{v} / dP \right) \right]^{\frac{1}{1+v}} + FZy \cdot \left[Cy \cdot \left(Y0^{v} / dY \right) \right]^{\frac{1}{1+v}}}$$

From these dependencies it is evident that the increase of initial probabilities and the reduction of levels of uncertainty increase the costs Z (dP, dY) (Fig. 2).

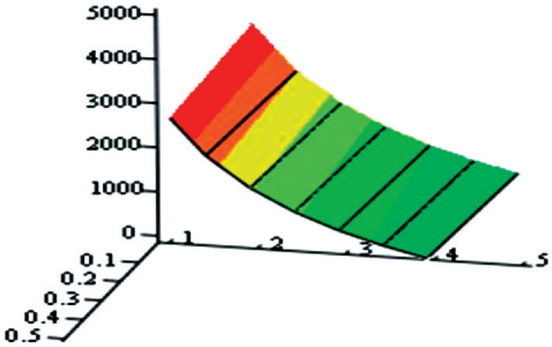

Fig. 2. Relationship between the increase of costs and the reduction of uncertainty levels in risk assessments

Without changing the adopted assumptions and taking eps=1, Cp=20, Cy=1, we will have

$$dP = 0.036\,,\ dY = 0.561 \text{ and } CS = 5.502 \times 10^{4}.$$

The level of a new guaranteed risk will make up

$$(P_0 + dP)\cdot(Y_0 + dY) = 11.02.$$

As we can see, the error of linearization in regard to the nominal risk and adopted limits in this case is also negligible (0.02).

To verify the analytical solution, some computational experiment has been carried out. Calculations of the optimal variations of risk factors were performed using the directive «Given» and the procedure «Minimise» of MathCad. Results of the solution practically (up to the machine representation of numbers) are the same. The same problem but in view of limitation in the form of the geometric sum of influence functions

$$\sqrt{(FZp\cdot dP)^2 + (FZy\cdot dY)^2} = eps$$

provides the same level of a guaranteed risk at higher values of risk factors, compared to the worst-case scenario

$$dP = 0.047\,,\ dY = 0.691 \text{ and } CS = 242.068.$$

The level of the guaranteed risk will make up

$$R_{г} = 11.317$$

The risk of non-fulfilment of the design functional task of AS can be defined as the product of the probability of a hazardous event by the size of damage [4]. The most important thing is to obtain a risk function taking into account the information resource state of AS. Dependences for the state of information resources (with exponentially distributed cyber attacks) and the distribution function of time for process execution in AS, as well as the mean damage are shown in Fig. 3.

Risk function in view of the state of AS information resources can be represented in the following form:

$$R(t) = \begin{cases} 0 \quad при \ \ t \le t[N(t) = РФЗ], \\ FR(t \le T_{фз})\cdot[РФЗ - N(t)] \quad при \quad t > t[N(t) = РФЗ], \end{cases}$$

where *FR(t)* is the distribution function of time of generating a set of actions to manage AS information resources; *N(t)* is the current AS information resource; РФЗ is the level of the design functional task; $T_{фз}$ is the time point when the current level of AS information resources reaches the level minimally necessary for the solution of a functional task.

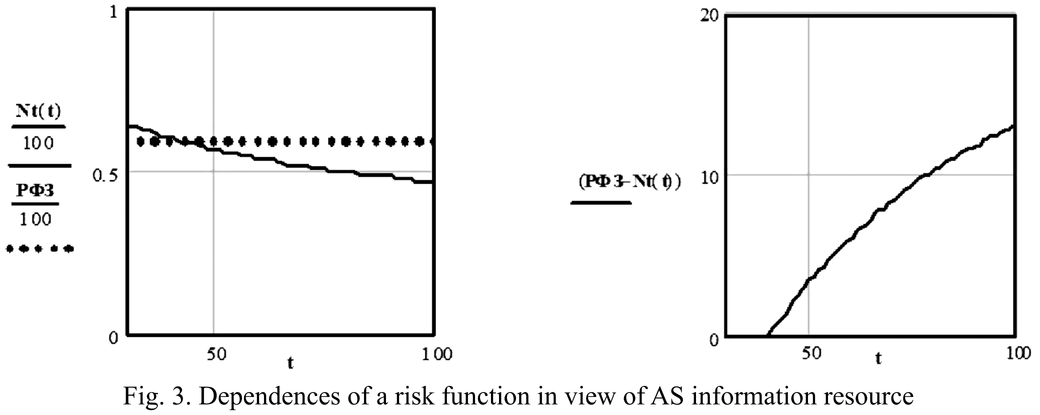

Fig. 3. Dependences of a risk function in view of AS information resource

Fig.4 shows functions of the average risk, including the risk relative to the design functional task for continuous AS under conditions of cyber attacks, and their lower and upper limits.

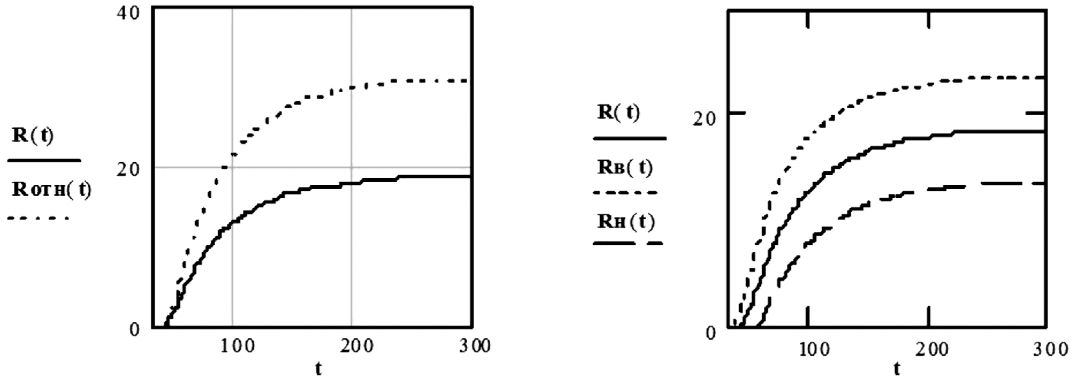

Fig. 4. Functions for the average risk of continuous AS application

Values of functions in Fig. 4 are defined by the following expressions

$$R_{\text{н}}(t)=\begin{cases}0 \quad \text{при} \quad t \le t\left[N_{\text{в}}(t)=P\text{Ф}3\right],\\ FR(t\le T_{\text{ф}3})\cdot\left[P\text{Ф}3-N_{\text{в}}(t)\right] \quad \text{при} \quad t>t\left[N_{\text{в}}(t)=P\text{Ф}3\right],\end{cases}$$

$$R_{\text{в}}(t)=\begin{cases}0 \quad \text{при} \quad t \le t\left[N_{\text{н}}(t)=P\text{Ф}3\right],\\ FR(t\le T_{\text{ф}3})\cdot\left[P\text{Ф}3-N_{\text{н}}(t)\right] \quad \text{при} \quad t>t\left[N_{\text{н}}(t)=P\text{Ф}3\right],\end{cases}$$

where Nн (t) and Nв(t) are the upper and the lower boundaries of a spread of AS information resources.

In practice, risk management of AS operation stability violations under conditions of cyber attacks is provided by

– Maintaining the required level of AS information resources with a priori given distribution of cyber attacks;

– Actively counteracting against sources of cyber attacks;

– Increasing the speed of computational processes of AS management and design functional tasks.

Therefore, we proposed a method for managing AS risks under conditions of cyber attacks based on analytical expressions for target functionality and tolerances of risk factors enabling us to make reasonable decisions on risk management of automated systems.

References

1. Volkov L.I. System safety and reliability. M. CIP RIA. 2003. p. 268.

2. Vasilenko V.V., Glukhov A.P., Kotyashev N.N. Risk management of application of designed systems under conditions of impacts / / Strategic stability, No.1, 2008. p. 39-46.

3. Rozenvasser E.N., Yusupov R.M. Sensitivity of control systems. Nauka. 1981. p. 464.

4. Shubinsky I.B. Functional dependability of information systems. Methods of analysis. – Ulyanovsk Regional Press "Printing House," 2012. p.296