**Scientific and Practical Cyber Security Journal (SPCSJ) 7(3): 11 – 16 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# MATHEMATICAL MODELS AND ALGORITHMS FOR DETERMINING TIME DECISION-MAKING IN THE CYBER DEFENSE SYSTEM

Volodymyr Khoroshko[1], Mykola Brailovskyi[2], Yulia Khokhlachova[1], Natalia S. Vyshnevska[1]

[1] National Aviation University, Kyiv, Ukraine
[2]Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

**ABSTRACT:** The article analyzes the literature, which shows the current lack of a unified approach to the comprehensive solution to the problem of synthesizing mathematical models and algorithms for determining the time of decision-making in the system of both protection and cyber protection of information. An analysis of the research stage was also carried out to determine the permissible terms of solving information-dependent problems of cyber information protection systems, taking into account the relationships between the directive terms of solving problems and the tasks of information dependencies between them, and determined the permissible intervals of processing and transmitting information over the network while ensuring the functioning of cyber information protection systems. Thus, the results that can be used in the development of effective algorithms for determining the time of decision-making based on mathematical models for decision-making support systems by the information cyber protection system, as well as for modeling complex technical systems and evaluating the effectiveness of the use of various information computing systems are given.

**KEYWORDS:** cyber security, cyber defense, cyber-attacks, cyber defense system, information protection, state protection, cyber space, communication channels.

## INTRODUCTION

Today, the issue of cyber defense as a component of the state's information security is extremely relevant for Ukraine and the international community.

It should be borne in mind that the use of cyberspace [1, 2] expands people's ability to communicate, promotes the development of information technology, research and innovation, and stimulates the development of industry and the economy. At the same time, the advantages of modern cyberspace inevitably lead to new threats to people, society, national and international security. Along with initiatives of natural (unintentional) origin, the number and power of cyberattacks motivated by the interests of individuals, groups, states and associations of states is growing.

In addition, it should be noted that the industry of informatization and communication, information services at the present stage of society's development is one of the most developed areas of the world society. It has made information security systems more relevant for information and communication technologies and for the processing, storage and transmission of information in the global cyberspace.

The great complexity and at the same time vulnerability of these systems and the entire cyberspace on which the global, national and regional community is based functionally depend on their stable and reliable operation and protection from information influences and cyberattacks.

Therefore, it is necessary to apply various methods of counteracting them and use mathematical methods of modeling, building and analyzing models of both cyberattacks and cyber defense.

Increasing the efficiency of mathematical modeling of cyber security systems for state information can be achieved by modeling both the complex system and its subsystems. This necessity stimulates the development of models and algorithms that allow solving complex problems of system management and information flow processing.

Regarding the construction of the initial distribution of the total load of subsystems and communication channels of cyber information protection systems (CIPS) not only of the state, but also of society and individual enterprises and organizations [3]. In addition, it is necessary to determine the

tolerance interval of the solution for each task of the integrated cyber information security system, taking into account.

Setting directive deadlines for solving problems; Interrelated information processing and transmission tasks. It should be noted that cybersecurity is a priority area of state policy in the development of electronic space and the formation of the information society in Ukraine. Cyber security (cyber defense) should be understood as the protection of the state's cyberspace, which ensures the sustainable development of the information society and the communication environment, timely detection, prevention and neutralization of cyber-attacks.

The objects of cyber defense include: Communication systems of all forms of ownership that process national information resources; Critical information infrastructure facilities. Cybersecurity in Ukraine is based on the following principles: Openness, accessibility, stability and security of cyberspace, development of the Internet and responsible actions in cyberspace; Public-private interaction, broad cooperation with civil society in the field of cybersecurity and cyber defense; International cooperation to prevent the use of cyberspace for illegal purposes. Determining the tolerance intervals of the solution is carried out in several stages. At the first stage, the directive deadlines for solving problems are linked to the real-time moments defined for the IPSS tasks to the technological goals of control and management, the duration of which is determined by the period of time during which the data obtained on solving the problems of managing the facility's cybersecurity system reflect the objective reality with the specified accuracy, which allows making the right decision on managing the facility's IPSS.

The second stage involves resolving the relationship between the policy deadlines for solving cybersecurity tasks. Directive terms regulate the time of the possible start and the required completion of the task on the network and are determined by external factors. The interconnection of the directive terms of solution is carried out taking into account the information links between the tasks that are determined in the process of cybersecurity of information and the analysis of the information and logical structure of the set of tasks of managing the cybersecurity of the object.

At the third stage, taking into account the interrelationships of the directive deadlines for solving tasks and the task of information dependencies between them, the permissible intervals for processing and transmitting information over the network are determined while ensuring the functioning of IPSS.

## PURPOSE OF THE WORK

The aim is to study the third stage to determine the acceptable timeframe for solving information-dependent tasks of IPSS.

## THE MAIN PART

Analysis of the literature shows that there is currently no single approach to a comprehensive solution to the problem of synthesizing mathematical models and algorithms for determining the time of decision-making in the system of both information protection and cybersecurity [4,5,6]. This problem is an unresolved part of the general problem of ensuring information security in integrated systems of technical protection and cybersecurity of information.

Let us consider the formulation and solution of this problem. Given: an interconnected subset of $Z_1$, consisting of $n$ tasks of information processing and transmission that involve the implementation of IPSI, requiring $N$ subsystems and $L$ communication channels $Z_1 = \{Z_j\}$.

The characteristics of each problem to be solved are known $Z_j$ - the labor intensity of the solution $W_j$ for information processing tasks and the amount of information transmitted $V_j$ for information exchange tasks via communication channels, the directive coordination of the terms of possible start $d_j^H$ and the required completion of the task $d_j^K$. The interconnection of tasks $Z_1$ is described by the set $X_j$ and $Y_j$ - respectively, the set of information inputs to the task $Z_j^{вх}$ and the set of information outputs from

$Z_j^{aux}$. It is required to determine for each , $Z_j \in Z_1$, $j = \overline{1,n}$ the following bounds of the admissible interval of its solution on the boundary of $t^H{}_j$ and $t^K{}_j$, that

$$\left[t_j^H, t_j^K\right] \subseteq \left[d_j^H, d_j^K\right]$$

And resolving all $Z$ within the permissible $\left[t_j^H, t_j^K\right]$ interval requires a minimum of costs to create and operate secure component of the network's technical means.

The mathematical formulation of the problem is as follows.

Identify the following, $t^H{}_j t^K{}_j$, which reach the minimum gradually mail functionality

$$C = \min_{t_j^H, t_j^K} \left\{ \sum_{e=1}^{E} \Theta_{1e} \sum_{i=1}^{N} \sum_{j=1}^{n} \left( \frac{W_j \Pi_{ji}}{t_j^K - t_j^H} \right)^{\beta_{1e}} + \sum_{q=1}^{Q} \Theta_{2g} \sum_{i=1}^{L} \sum_{j=1}^{l} \left( \frac{N_j \eta_j}{t_j^K - t_j^H} \right)^{\beta_{2q}} \right. \quad (1)$$

With the following restrictions

$$d_j^H - t_j^H \le 0, \; j = \overline{1,n}, \quad (2)$$

$$t_j^K - d_j^K \le 0, \; j = \overline{1,n} \quad (3)$$

$$t_j^H - t_j^K \le 0, \; j = \overline{1,n} \quad (4)$$

$$t_j^K - \min_a \left\{ t_a^H \mid a \in Y \right\} \ge 0, \; j = \overline{1,n} \quad (5)$$

Constraints (2) and (3) take into account the given directive deadlines for solving problems $Z_{j\,j}$. Constraint (4) sets the conditions for a non-zero length of the tolerance interval of the solution $Z_j$ . Constraint (5) imposes the requirement that the tolerance intervals of information-related tasks should not overlap if the j-th task is distributed for processing to the i-th subsystem, in the main case if the i-th task of information exchange of the l-th communication channel

$$\Pi_{ji} = \begin{cases} 1 \\ 0 \end{cases}$$ if the j-th task is distributed for processing to the i-th subsystem

, in the main case

And

$$\Pi_{ji} = \begin{cases} 1 \\ 0 \end{cases}$$ if the i-th task of information exchange of the l-th communication channel

, in the main case

Criterion C in (1) describes the total present value costs of creating and operating the technical means of a network designed to serve the tasks $Z_1$. E and $\Theta_{1e} > 0$; $\Theta_{1e} > 0$; ; $\beta_{1e} \ge 0$ $\beta_{2\,eq} \ge 0$ are constants.

Tasks (1)-(5) belong to the class of nonlinear mathematical programming problems. Known methods of nonlinear programming theory can be used to solve them. A characteristic feature of problems (1)-(5) is its large dimensionality, which is determined by the number of problems that are solved on the network and are in information interconnection. One of the effective approaches to solving nonlinear optimal problems of high dimensionality is the use of approximation methods of nonlinear programming theory [9, 10, 11], the essence of which is that the solution of the final nonlinear problem is carried out as a result of solving a sequence of problems of a simpler type, which require much less computational effort than the original problem.

Linear approximation is not always effective, as it only gives you a fairly approximate value.

Recently, scientific papers have proposed an approach to eliminate this drawback: solvable auxiliary quadratic problems. The minimization method used in [12, 13] occupies a special place among all such methods. This is due to the fact that, unlike other methods of my class, it converges from any initial approximation and does not require assumptions about the convexity of functions, does not require

strict positive definiteness of the matrix of second derivatives of Lagrange functions, and has a fairly simple structure of the auxiliary quadratic problem.

In general, the linearization method has a linear rate of convergence. However, there is a modification of the method [14,15], for which, at a considerable distance from the extremum point, the rate of ascent is linear, and at sufficient proximity to it, it is quadratic.

The peculiarity of solving quadratic problems is that they take into account only those constraints in which the violation of admissibility is the greatest [13]. This feature reduces the dimensionality of auxiliary problems and thereby reduces the computational complexity of the original nonlinear problem.

The advantages of the linearization method discussed above determine the definition of acceptable intervals in the statement of the problem (1)-(5).

For the algorithm of the linearization method to work, it is necessary to choose an initial approximation to the solution $t_j^K(0)$, $j=\overline{1,n}$ that satisfies the system of inequalities (2)-(5). Let the set of interconnected problems $Z_1$ be divided into R - information ranks by nr problems in the *r* -th rank, $r=\overline{1,R}$. The algorithm for the initial approximation is as follows:

Step 1 $r:=1$

Step 2 $j:=1$

Step 3 $t_j^H(0):=d_j^H+\Delta t\ t$

Step 4 $t_j^K(0):=t_j^H(0)+\Delta t$

Step 5 $j:=j+1$

Step 6 If $j\le n_r$, go to step 3, otherwise go to step 7

Step7 $r:=r+1$

Step 8 If $r\le R$, go to step 9, otherwise go to step 17

Step 9 $j:=j+n_{r-1}$

Step 10 $t_{\min}^H:=\min_a\left\{t_a^H(0)\mid a\in X_j\right\}$

Step 11 $t_j^H:=t_{\min}^H+2\Delta t$.

Step 12 If $d_i^H>t_j^H(0)$, go to Step 13, otherwise 14.

Step 13 $t_j^H(0):=d_i^H+\Delta t$

Step 14 $t_j^K(0):=t_j^H+\Delta t$

Step 15 $j:=j+1$.

Step 16 If $j\le n_r$, go to Step 10, otherwise go to Step 7.

Step 17 End.

The choice of the value Δ*t* is carried out depending on the task of the directive terms of solution $d_j^H$, $d_j^K$, $j=\overline{1,n}$.

Let $t_j(0)=\left\{t_j^H(0),t_j^K(0)\right\}$ and , $\bar{t}(0)=\left\{t_j(0)\right\}$, $j=\overline{1,n}$ be the initial approximation to the solution obtained by the algorithm described earlier, and let the accuracy of *E* , 0<E<1, be given. Consider the work of the algorithm of the linearization method [9] at the k-th step, when we have already obtained the *k-th* approximation $\delta>0$ to the solution *(k)*.

The construction of the *(k+1)*th approximation $\bar{t}(k+1)$ is carried out as follows:

1. The task of quadratic programming

$$\min_{\overline{P}}\left\{\left[\overline{C}^T(\bar{t}(k)),\overline{P}\right]+\frac{1}{2}\|\overline{P}\|^2\right\}. \qquad (6)$$

$\left[\overline{\varphi_S}(\bar{t}(k)),\overline{P}\right]+\varphi_S\left[\bar{t}(k)\right]\le 0$, $s\in S_\delta[\bar{t}(k)]$, is decided in relation to $\overline{p}$.

Here, $S_\delta(\bar{t}) = \left\{ s \in S : \overline{\varphi_S}(\bar{t}) \geq s^{\max} \in S \ \varphi_s(t) - \delta \ \right\}$, $\delta > 0$

$\Phi = \left\{ \overline{\varphi}_s(\bar{t}) \right\}$ - a set of functions such as

$$\overline{\varphi}_S = (t) \begin{cases} d_S^H - t_{S_1}^H, S = \overline{1,n}, \\ t_{S-n}^K - d_{S-n}^K, \ S = (\overline{n+1),2n}, \\ t_{S-2n}^K - t_{S-2n}^K, \ S = (\overline{2n+1),3n}, \\ t_{S-3n}^K - \min\limits_{a} \ \left\{ t_a^H \mid a \in \frac{1}{5} - 3n \right\}, \ S = (3\overline{n+1),4n}; \bar{t} = \left\{ t_j \right\}, t_j = \left\{ t_j^H, t_j^K \right\}, \ j = \overline{1,n}; \end{cases}$$

$\| \overline{p} \|$ is euclidean norm of a vector $\overline{p}$.

2. We find the first value of $S = 0,1,...,$ at which the following inequality is satisfied

$$\overline{\varphi}\left[ \bar{t}(k) + \frac{1}{2^S} \overline{p}(k) \right] + N \max_{s \in S} \overline{\varphi}_S \left[ t(k) + \frac{1}{2^S} \overline{p}(k) \right] \leq \overline{\varphi}\left[ \bar{t}(k) \right] + N \max_{s \in S} \overline{\varphi}_S \left[ \bar{t}(k) \right] - \frac{1}{2^S} \varepsilon \| \overline{p}(k) \|^2$$

If this inequality was first used in $S = S_0$, we note that

$$a(k) = 2^{-S_0}, \bar{t}(k+1) = \frac{1}{t}(k) + (k)\overline{p}(k)$$

Thus, at each step of the algorithm, the inequality is performed

$$\overline{\varphi}\left[ \bar{t}(k+1) \right] + N \max_{s \in S} \overline{\varphi}_s \left[ \bar{t}(k) + 1 \right] \leq \overline{\varphi}\left[ \bar{t}(k) \right] + N \max_{s \in S} \overline{\varphi}_s \left[ \bar{t}(k+1) \right] - a(k) \varepsilon \| \overline{p}(k) \|^2 \quad (7)$$

In [11], we show that the choice of $a(k)$ at each iteration takes a finite number of halving of the unit, and we prove the convergence of the algorithm. In particular, we prove that if the objective function and constraints are convex, the algorithm converges in a finite number of steps for any $a < 0$.

All the constraints (2)-(5) are linear, so they are convex. The above analysis of the objective function (1) shows that it is a convex function. Thus, for the problem (1)-(5), the linearization algorithm converges in a finite number of steps for any $a < 0$.

When using the linearization method, the main operation requiring significant computational costs is the solution of the quadratic problem (6). When choosing a method for solving it, it should be borne in mind that to control the correctness of the choice of the constant *N* in (7) when solving (6), it is necessary to obtain the corresponding Lagrange multipliers $\overline{U}(\overline{P})$ [11]. Therefore, when solving problem (6), it is advisable to move to a dual problem, which has the form

$$U = \left\{ \overline{U}^T \cdot G\overline{U} + h^T \overline{U} \mid \overline{U} \geq 0 \right\},$$

(8)

Where $G = A \cdot \overline{A}^T$, $\overline{h}^T = A\bar{b} + \overline{C}^T \left[ \bar{t}(k) \right]$; $A$ is amatrix, $S$ is a string containing the components of the vector $\overline{\varphi}_S \left[ \bar{t}(k) \right]$, $\bar{b}$ is a vector, $\overline{S}$ is a component equal to the value of the function $\overline{\varphi}_S \left[ \bar{t}(k) \right]$.

To solve problem (8), it is advisable to use an iterative algorithm that represents some modification of the Gauss-Seidel method [16, 17]. The choice of this algorithm is due to the fact that, firstly, it is quite simple to implement on a computer, and secondly, its structure, calculation errors at individual iterations do not affect the convergence of the iterative process as a whole.

This algorithm for solving problem (8) has the following form

$$U_i^{(n+1)} = \max(0, \omega_i^{(n+1)}), \quad (9)$$

$$\omega_i^{(n+1)} = \frac{1}{g_0} \left( \sum_{j=1}^{i-1} g_{ij} U_j^{(n+1)} + h_i + \sum_{j=i+1}^{m} g_{ij} U_j^n \right), \quad (10)$$

Where $U_i$ and the component of vector $\overline{U}$.

$n$ - iteration number; $g_{ij}$ - element of the matrix $G$;

$m$ - the dimension of the vector $\overline{U}$ .

The algorithm described is implemented in the form of a set of application programs for analyzing the effectiveness of algorithms for determining the decision-making time of cyber security systems.

## CONCLUSION

Overall, these results can be used to develop effective algorithms for determining decision-making time based on mathematical models for decision support systems for cyber information security, as well as for modeling complex technical systems and evaluating the efficiency of using various information and computer systems.

In addition, the results of the study allow us to quantify the effectiveness of various computing systems and make it possible to choose the best system based on a specific practical task.

## REFERENCES

1. Hryshchuk R.V. Fundamentals of cyber security / R.V. Hryshchuk, Y.G. Danik - Zhytomyr: ZhNANEU, 2016. - 636 p.

2. Brailovskyi M.M. Information security technologies / M.M. Brailovskyi, S.V. Zybin, I.V. Piskun, V.O. Khoroshko, Y.E. Khokhlachova - K: CC "Komprint", 2021. - 296 p.

3. Khoroshko V.O. Scientific tasks of synthesizing the organizational and technological scheme of creating software for computer networks with limited access / V.O. Khoroshko, N.F. Kazakova // Information Protection, No. 4, 2009.

4. Kozyura V.D. Choice of the moment for the operation of influence on information / V.D. Kozyura, I.V. Pikun, V.A. Khoroshko // Information security: human, society, state, No2, 2011.

5. Dakhno N.V. Calculation of the time of efficiency of the decision-making process in information security systems / N.V. Dakhno, E.O. Tiskina, V.A. Khoroshko // Modern Information Technologies in the Field of Security and Defense, No. 2 (5), 2011.

6. Zabolotsky V.P. Mathematical models in management / V.P. Zabolotsky, A.A. Ovodenko, A.G. Stepanov - St. Petersburg: St. Petersburg State University of Management and Administration, 2001.

7. Samarskiy A.A. Mathematical modeling: Ideas, Methods, Examples. 2nd ed. / A.A. Samarskiy, A.P. Mikhailov. - M: Fizmatlit, 2001. - 316 p.

8. Kelton V. Simulation modeling, 3rd ed: Piter, K: BHV Publishing Group, 2004. - 847 p.

9. Feldman L.P. Numerical methods in information / L.P. Feldman, A.I. Petrenko, O.A. Dmitrieva - K: BHV Publishing Group, 2006. 480 p.

10. Mathews D.G. Numerical methods / D.G. Mathews, K.D. Fink: SPb: K: Williams, 2001. - 713 p.

11. Samarskiy A.A. Numerical methods of mathematical physics / A.A. Samarskiy, A.V. Gulik - Moscow: Scientific World, 2003. 316 p.

12. Verzhbitskiy V.M. Osnovy numeral'nykh metodov [Fundamentals of numerical methods]: Vyssh.shk., 2002. - 840 p.

13. Hemming R.V. Numerical methods for scientists and engineers. 2nd ed: Nauka, 1998. 402p.

14. Tomashevsky V.M. Modeling of systems / V.M. Tomashevsky. - K: BHV Publishing Group, 2007. - 352 p.

15. Tomashevsky V.M. Solving practical problems by computer modeling / V.M.Tomashevsky, O.G.Zhdanov, O.O.Zholdakov - K: Korniychuk, 2001. - 267 p.

16. Knut D.E. The art of programming. - Vol. 2. Computed algorithms. 3rd ed: Izd.dom. "Williams, 2001. - 832 p.

17. Ryzhikov Y.I. Simulation modeling theory and technology / Y.I. Ryzhikov: Korona; M: Altex, 2004. - 384 p.