UDC 32.973.202 (004.8)

DYNAMIC MANAGEMENT OF CYBERSECURITY RESOURCES BASED ON GENETIC ALGORITHMS

Akhmetov Bakhytzhan, Lakhno Valeriy, Adilzhanova Saltanat

Kazakh National Pedagogical University named after Abai[1],
National University of Bioresources and Occupational Sciences of Ukraine[2],
Al-Farabi Kazakh National University[3]
[1]b.akhmetov@abaiuniversity.edu.kz, [2]lva964@nubip.edu.ua,
[3]asaltanat81@gmail.com

The report examines methods, models and information technologies for the dynamic management of cybersecurity resources. The relevance of the study is determined by the need to optimize the indicators of information security tools of the object of informatization (OBI) in the conditions of dynamic confrontation with the attacking party. The solution to the problem is seen in the optimal distribution of limited financial resources of the OBI management between the objects of protection, taking into account the actions of the attacker.

The problem of dynamic resource management of the OBI protection side is not only a purely technical task, which is solved by increasing the number of protection components in the cybersecurity circuits (KB) of the OBI. But it's also a management challenge. Moreover, the second component of the tasks is associated with such a concept as information security management (IS) and KB, the main task of which is to optimize not only technical, but also economic indicators of the effectiveness of the functioning of information security tools (SIR) for OBI [1].

The criterion of optimality can be one (or several) indicators of information (cybernetic) security - the amount of damage from the implementation of information threats, total costs, which include damage from information leakage and the cost of its protection, profit from investments in information protection, etc. At the same time, it is quite difficult, and often impossible, to achieve optimal values of various indicators due to the inconsistency of their requirements. As a result, we come to a multi-criteria problem [2].

The solution of the task is complicated by a number of reasons. The main one is due to the fact that the search for the optimal solution is conducted in conditions of uncertainty, when the actions of the opponent can be assumed only with a certain probability, and sometimes it is impossible at all.Under these conditions, the search for the optimal distribution of limited resources between the objects of information protection (IR) is possible through the use of game-theoretic methods and taking into account the dynamics of changes in conditions, which will reduce the vulnerability function of the objects of protection to a minimum [3].

The winnings of each side depend on the opponent's strategies and are determined by the objective function. $o(h,d)$. The objective function for the attacker and the defense side can be as follows: $o(h_k, d_k) \to \max$. $o(h_k, d_k) \to \min$.

The amount of damage caused can be estimated, for example, by the cost of an information resource (IR). The amount of damage will depend on the distribution of the resources of the parties.

The strategy of the attacker (attackers) is to distribute his resources between objects in different ratios:

$$\{h_{ik}\} = (h_1, h_2, ..., h_l), \sum_{k=1}^{l} h_k = H, h_k \geq 0, \quad (1)$$

where is $k -$ object number of protection $(k = \overline{1,l})$, $h_k -$ costs (resources) for the implementation of threats at the facility k; l -is the number of objects of protection, H - is the total number of attack resources; i – the current number of the object of attack.

Similarly, the defence applies its resource allocation strategy:

$$\{d_{jk}\} = (d_1, d_2, ..., d_l), \sum_{k=1}^{l} d_k = D, d_k \geq 0, \quad (2)$$

where is $d_k -$ costs (resources) for the implementation of protection on site k; D – total number of protection resources; j – the current number of the object of protection.

For the selected game model, the target function expresses the damage caused by the implementation of threats and has the form:

$$o(h_k, d_k) = \sum_{k=1}^{l} o_k(h_k, d_k) = \sum_{k=1}^{l} g_k p_k v_k(h_k, d_k), \quad (3)$$

where is $k = \overline{1,l} -$ Object number for protection;

$h_k, d_k -$ accordingly, resources of attack and defence;

$g_k -$ relative value of IR on $k -$ object;

$p_k -$ the likelihood of an attack on a IS facility;

$v_k(h_k, d_k) -$ vulnerability $k -$ IR object is considered as a probability of a successful attack and depends on the costs of attackers and the cost of protecting the object.

Values $o(h,d)$, $o_k(h,d)$, g_k are attributed to the entire value of the IR.

The first step is to find the parameter values and the form of the dependencies that are included in the objective function (3).

When establishing dependencies $v(h,d)$ the following considerations were taken into account. The probability of a successful attack is directly proportional to the cost. h to carry out the attack and inversely proportional to the costs d to protect the object. Therefore, variables h,d must be included in the expression for $v(h,d)$ as an attitude $r = h/d$.

It is clear that dependencies $v(h,d)$ must meet the following conditions:

at $r = (h/d) \to 0,\ v(h,d) \to 0$; at $r = (h/d) \to \infty,\ v(h,d) \to \infty.$

These conditions are satisfied by the power functions of the species:

$$v(h,d) = r^n / (r^n + a), \tag{4}$$

where *a* and *n* are constants that determine the position and shape of the curves.

The solution of the objective function (3) in the analytical form is very difficult. Its solution is greatly influenced by vulnerability $v(h,d)$ object, which is considered as the probability of a successful attack and depends on the costs of the attackers and the cost of protecting the object. However, knowing the values of the parameters and the form of dependencies that are included in the expression for vulnerability (4), we can replace the procedure for solving the objective function with finding the parameters *a* and *n*.

The task of establishing the form of dependence of the probability of a successful attack on the ratio of attack and defense resources is quite complex and is solved separately for each specific system. In our case, the form of dependence was established on the basis of expert assessment of specialists in the field of information protection of Ukraine and the Republic of Kazakhstan and defined as a power function of the species (4). At $n = 1$ it expresses a fractional-linear dependence, with $n > 1$ – fractional-nonlinear [4].

The following is the initial data for solving this task on the example of a parameter study , which affects the degree of vulnerability of the IR to the OBI.

Consolidated list of works to ensure the protection of information on the OBI (to determine the maximum value of *a)*

1. Design, development and deployment of an integrated SPI (A).
2. Improvement of the information security system (ISS) (B).
3. Identification of information security incidents, incident response, risk forecasting for OBI (S).
4. Minimization of connections between individual objects of IR and unification of components of IR (D).

5. Development of organizational measures of IR, corresponding to the specifics of the business processes of OBI (E).

Grouping of allocated resources by object of expenditure (types of resource investment in IR and KB)

1. Material and financial costs for IR (MFC).
2. Human resources involved in projects to provide IR and KB OBI (HR).
3. Costs of project management in the field of IR and CC OBI (CM).
4. Other costs for the provision of IR and CC OBI (RS).

Competitive advantages from the implementation of events IR and CC for OIB (optimality criteria)

1. Improving competitiveness and new markets (COP, *k=1*).
2. Development of innovations and introduction of digital technologies in business processes (IN, *k=2*).
3. Reduced IT costs (RI, *k=3*).

The optimality criterion in the process of determining the parameters can be described as:

$$F_k = \sum_i \sum_j I_j \cdot E_{ijk} \cdot X_{ijk} \xrightarrow{\sim} \max,$$

where *k* is the number of the optimality criterion; *k=1,2,3*;

$I_j -$ priority (importance) in the chosen optimal option for the allocation of resources of the defense side, $\sum I_j = 1;$

$i = 1(A),2(B),3(C),4(D),5(E) -$ types of work type from the list of works, may vary depending on the characteristics of the OBI;

$j = 1$ for MFC, $j = 2$ for HR, $j = 3$ for storage, $j = 4$ for RS – types of investment investments (resources);

$X_{ijk} -$ variable, equal to 1, if the work (i) from the list of works is used to implement the investment investment (j). Otherwise, we accept – 0;

$E_{ijk} -$ work efficiency of the type (i) from the list of works that are performed for the implementation of the investment (j) that provides an optimality criterion;

$\xrightarrow{\sim} -$ non-strict achievement of the optimal parameter value *a*.

Restrictions on the allocated resources available to the company can be set as follows:

$$Q = \sum_i \sum_j I_j \cdot l_{ijk} \cdot X_{ijk} \le A_j,$$

where is l_{ijk} – resource costs (j) (or labor intensity), which are associated with the performance of work of the type (i) that provides an optimality criterion k;

A_j – resource investment restriction (j), which are related to the performance of work of the form (i) that provides an optimality criterion k.

The constraints that determine the structure of the solution of the problem (or the arrangement of values 0 and 1 in the decision matrices) are described below.

Restriction $\sum_i X_{ijk} \geq 1.$ means that in the direction of resources, for

At least one of the works of the optimality criterion is used according to the list of works:

Restriction $\sum_j X_{ijk} \geq 1.$ means that in the course of operation of the (j) for $k-$ th criterion of optimality, resources (i) use at least once.

Restriction $\sum_k X_{ijk} \geq 1.$ means that any kind of work of the type (i) in any direction of resource allocation (j) must participate in the formation of at least one $k-$ the optimality criterion [5].

To solve the problem of finding rational parameters *a* and *n* that are part of the objective function, it is proposed to use a modified genetic algorithm. This algorithm, along with their known advantages, evaluates the fitness of the chromosome to solve the multi-criteria problem of optimizing the allocation of resources of the defense side with fuzzy relationships (calculates the attractiveness of the solution) based on the Bellman–Zadeh principle. This makes it possible to solve the optimization problem under the condition of the evolution of the system from the current state to some finite one and, accordingly, to move from solving the original multi-step optimization problem to the sequential solution of several one-step optimization problems, for example, by determining the parameters *a* and *n*.

Forsituations, where the number of ICS nodes is large enough, it is quite a laborious process to solve in parallel the problem of selecting, optimiIRng and redistributing all the resources of the defense side tolassic methods. Therefore, it is proposed to apply a composite genetic algorithm to solve this problem. The essence of its application is that at the first stage a genetic algorithm (GA) is involved in solving the problem, and at the second stage, the solution found with the help of GA can be improved by the method of branches and boundaries (MGA) [6].

In the course of computational experiments, a comparative analysis of the composite algorithm (GA + MGA) with the classical GA, "greedy" and the exact brute force algorithm was carried out. To evaluate the above algorithms, test sets from 5 to 150

items (SIR) in a set were formed. 5 series of 30 experiments per series were conducted, a total of 150 computational experiments. Computational experiments were performed on a PC with an Inte*l*7 9750H processor (2.6 – 4.5 GHz).

The expected solutions, which were obtained using the exact method of full search, turned out to be more accurate. But the operating time of such an algorithm, even taking into account the use of *i*7 processors, is 17-25 times greater than for GA or GA + MVG. It was found that the composite genetic algorithm is characterized by a sufficiently high efficiency and speed. The time spent on solving the problem when using it is about 16-25 times less compared to the indicators of the method of branches and boundaries. The greedy algo rhythm issignificantly inferior to both the GA and the method of branches and boundaries in terms of adaptability to solving a multi-criteria optimization problem, taking into account the restrictions imposed and the number of variables.

Literature

1. Akhmetov, B., Lakhno, V., Akhmetov, B., &Alimseitova, Z. (2018). Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity. In Proceedings of the Computational Methods in Systems and Software (pp. 162–171). Springer, Cham.

2. Sviridov, V. I., & Moiseev, S. I. (2019). Mathematical models of the optimal distribution of protective resources by sources of information threats. Bulletin of the Voronezh Institute of High Technologies, (1), 110-112.

3. Grischuk, R. V. (2012). The use of differential games to optimize control in information security systems / Grischuk R.V., Khoroshko V.A., Khokhlacheva Yu.E. Modern information protection (2), pp. 21–26.

4. Akhmetov, B. , Lakhno, V. , Yagaliyeva, B. , Oshanova, N. , Adilzhanova, S. Conceptual Diagram of An Intelligent Decision Support System in the Process of Investing in Cybersecurity Systems. Journal of Theoretical and Applied Information Technologythis link is disabled, 2021, 99(18), pp. 4297–4310.

5. Lakhno, V. , Adilzhanova, S., Kryvoruchko, O., Desiatko, A., Buriachok, V. Allocation of Organizational and Financial Resources of the Information Protection Side Using a Genetic Algorithm. Lecture Notes in Networks and Systems, 2021, 228, pp. 41–53.

6. Lakhno, V., Bereke, M., Adilzhanova, S., Desiatko, A., Palaguta, K. Genetic algorithm for solving the problem of scaling a cloud-oriented object of informatization. Journal of Theoretical and Applied Information Technology, 2022, 100(7), pp. 1693–1705.