Peculiar Properties of Creating a System of Support to Make Anti-Crisis Decisions by Experts of the Situational Center at the Cyber Protection Object

Vadym Tiutiunyk [1], Olha Tiutiunyk [2], Oleh Teslenko [3] and Natalia Brynza [4]

[1]*National University of Civil Defence of Ukraine, Chernyshevska Str., 94, Kharkiv, 61023, Ukraine*
[2,3,4]*Simon Kuznets Kharkiv National University of Economics, Science ave., 9-A, Kharkiv, 61166, Ukraine*

Abstract

Considering the uncertainty of the parameters affecting the conditions for the normal functioning of the cyber protection object, it is proposed to create a support system for making anti-crisis decisions by the experts of the situational center, which is an integral part of the information security system of the cyber protection object. The basis of the information security system of a cyber protection object shall be a classical control loop that ensures the collection, processing and analysis of information, as well as modeling the development of information danger at the cyber protection object and the development and implementation of anti-crisis management to prevent the emergence of threats to information circulating during the functioning of the cyber protection object, and also elimination or minimization of their consequences.

In the study, the risk indicator for information circulating during the functioning of a cyber protection object is the summation between the risk indicators of information disclosure and information leakage, as well as the risk indicator for computer information circulating during the functioning of the cyber protection object. The indicator of the risk of information leakage includes indicators of the risk of information leakage through technical channels, information leakage through communication channels, speech information leakage, as well as information leakage, shown information. The risk indicator for computer information includes indicators of the risk of loss and alteration of information, as well as obtaining unauthorized access to information.

In the context of untimely, incomplete and suboptimal information concerning the condition of information security of the cyber protection object, to solve the problem of multi-criteria optimization for the formation of alternatives to anti-crisis decisions by the experts of the situational center, in the study, firstly, the methods of obtaining initial information about the advantages of the on traditional heuristic procedures of expert evaluation, and concerning formal methods of comparator identification. It is shown that regardless of the method of obtaining the initial information and the form of its presentation, the most adequate is the interval assessment of the preferences of the decision maker. Secondly, a model of a multicriteria scalar assessment of the usefulness of feasible alternative solutions has been synthesized. The presented results represent the scientific basis for the development of a support system for making anti-crisis decisions in critical situations by experts of the situational center to ensure the appropriate level of information security of the cyber protection object.

Keywords

cyber protection object, information security system, situational center, anti-crisis decision support system, multi-criteria, uncertainty of initial information

III International Scientific And Practical Conference "Information Security And Information Technologies", September 13–19, 2021, Odesa, Ukraine
EMAIL: tutunik_v@ukr.net (A. 1); tutunik.o@ukr.net (A. 2); tov1967@meta.ua (A. 3); natalia.brynza@hneu.net (A. 4)
ORCID: 0000-0001-5394-6367 (A. 1); 0000-0002-3330-8920 (A. 2); 0000-0003-3105-9323 (A. 3); 0000-0002-0229-2874 (A. 4)

1. Introduction

Cyber protection objects (CPO) in the state are the following: 1) communication systems of all forms of ownership, in which national information resources are processed and/or used in the interests of state authorities, local authorities, law enforcement bodies and military formations formed in accordance with the law; 2) objects of critical information infrastructure; 3) communication systems that are used to meet public needs and/or implement legal relations in the areas of electronic government, electronic government services, electronic commerce, electronic document management [1-3].

The creation of an effective information security system of the CPO requires the inclusion of a subsystem of situational centers, rigidly interconnected at the information and performance levels for making appropriate anti-crisis decisions in solving various functional monitoring tasks, preventing the emergence of threats to information circulating during functioning of the CPO, as well as eliminating or minimizing their consequences [4-7].

One of the topical directions to create a subsystem of situational centers in the information security system of the CPO is the development of a justification methodology, under the uncertainty of initial information for experts of the system of situational centers, optimal anti-crisis solutions to prevent the emergence of threats to information circulating in the process of functioning of the CPO, as well as to eliminate or minimize their consequences.

An obligatory stage in the functioning of the system of situational centers is decision making. At the same time, not only incorrect, but also ineffective decisions lead to losses or irrational use of financial, time, labor, energy and other resources when managing the processes of prevention and elimination of emergency situations. In this regard, the problem of developing a scientifically grounded methodology to make effective decisions is one of the urgent scientific problems.

According to V.M. Hlushkov, the necessary conditions for the effectiveness of decisions are their timeliness, completeness and optimality. The listed requirements are contradictory and their satisfaction is connected with serious difficulties.

Provision the completeness (complexity) of decisions requires the fullest possible consideration of internal and external factors affecting decision-making, a deep analysis of their interrelationships, which leads to increase in the dimension of the decision-making problem, its multicriteria. In turn, this leads to increase in the uncertainty of the initial data, which is due to the incompleteness of knowledge about the relationship of factors and, as a consequence, its inaccurate description, the impossibility or inaccuracy of measuring some factors, random external and internal influences, etc. An additional complication is in the fact that uncertainties are heterogeneous and can be represented as random variables, fuzzy sets or simply interval values.

Thus, an increase in the efficiency of decisions made is connected with the need to solve multicriteria optimization problems in conditions of uncertainty.

The traditional, widespread approach to solving such problems, based on their heuristic simplification, determinization as a means of removing uncertainty, becomes less and less effective as the tasks become more complex and the significance of solutions increases [8].

In these conditions, it is extremely important to develop formal, normative methods and models for a comprehensive solution to the problem of decision-making in conditions of multi-criteria and uncertainty.

In this direction, principal, fundamental results have been obtained [9,10, 15-17], however, the only solution to the problem is far from completion and the continuation of research in this direction is undoubtedly relevant both in theoretical and applied aspects for the development of a substantiation methodology, under conditions of uncertainty in the input information for experts of the system of situational centers, optimal anti-crisis solutions to ensure the required level of safety for functioning of the CPO.

2. Peculiar properties of the situation center performance as a component of the support system for anti-crisis decision-

making at the cyber protection objects

The situational center while operating in the information security system of the CPO shall, in accordance with the data in Fig. 1, ensure the collection, processing and analysis of information, as well as modeling the development of information threat to the CPO and the development and implementation of anti-crisis management to prevent the emergence of threats to information circulating during functioning of the CPO, as well as to eliminate or minimize their consequences.

Functioning which is shown in Fig. 1, schemes in the conditions of completeness of the initial information and the presence of one partial criterion for assessing the set of feasible solutions does not present difficulties in substantiating optimal anti-crisis solutions. On the other hand, modern problematic situations are characterized by incompleteness of knowledge (uncertainty) of the initial data and many particular evaluation criteria. Thus, the traditional approach based on the decomposition of the problem into two socalled independent problems – multiobjective optimization in deterministic, that is, without concidering uncertainty, formulation and decision-making under uncertainty for a scalar objective function in modern conditions, does not meet the requirements of practice under accuracy and efficiency.

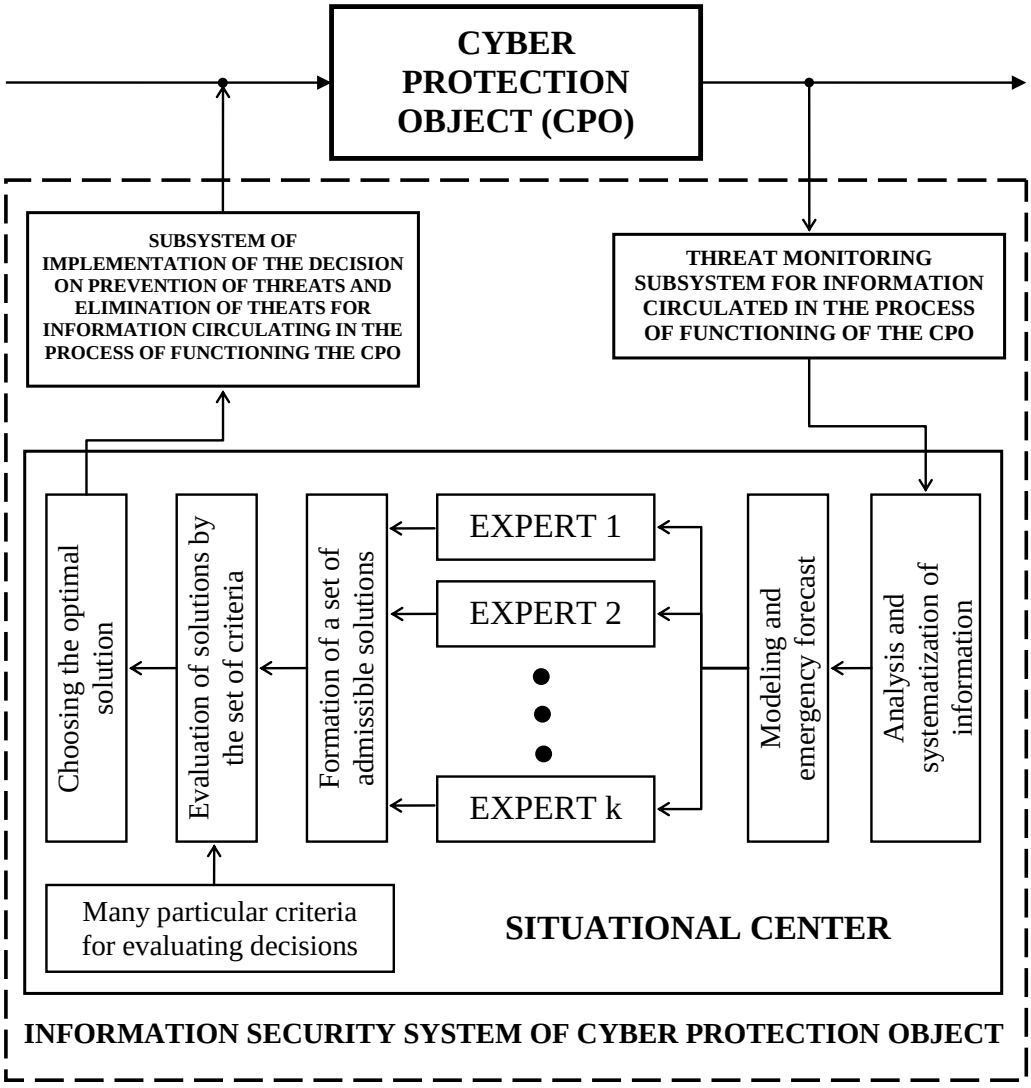

Figure 1: Functional scheme of substantiation of optimal anti-crisis solutions to ensure the appropriate level of security of the cyber protection object, under uncertainty of input information for experts of the situational center

This is due to the fact that the problem of multicriteria optimization is incorrect, because it allows to determine the solution only with precision in the field of compromise solutions, and its regularization to determine a single solution based on generalized multifactor scalar estimation, it is based on poorly structured, subjective expert assessments, the determination of which leads to large errors. On the other hand, methods of decision-making under the uncertainty under scalar estimate and the expected effect, without considering its multicriteria, are also not adequate. Therefore, there is the need to develop a methodology for comprehensive solutions to the problem of decision-making, considering the multi-criteria and incomplete uncertainty of the original data.

3. Risk assessment of threats to information circulating during the cyber defense object functioning

Based on the basic postulates of the risk-oriented approach, the risk indicator for the information circulating in the process of functioning of the CPO shall be represented as [18]:

$$R_{CPO}^{Inf.} = \sum_{i=1}^{3} R_{CPO_i}^{Inf.}, \quad (1)$$

where $R_{CPO_1}^{Inf.}$ – is a risk indicator for information circulating during functioning of the CPO, which is characterized by the disclosure of information; $R_{CPO_2}^{Inf.}$ – is a risk indicator for the information circulating in the process of functioning of the CPO which is characterized by information leakage; $R_{CPO_3}^{Inf.}$ – is a risk indicator for computer information circulating during the functioning.

The components of risk for the information circulating in the process of functioning of the CPO are presented in Fig. 2. The risk components for the information circulating in the process of functioning of the CPO are calculated by the formula:

$$R_{CPO_{i.j}}^{Inf.} = P_{CPO_{i.j}}^{Inf.} U_{CPO_{i.j}}^{Inf.}, \quad (2)$$

where $P_{CPO_{i.j}}^{Inf.}$ – is assessment of the probability of exceeding the normative indicator for the j-th aspect of the i-th process of danger for the information circulating in the process of functioning of the CPO; $U_{CPO_{i.j}}^{Inf.}$ – is assessment of the damage from exceeding the normative indicator of the impact of the j-th aspect of the i-th process of danger for the information circulating in the process of functioning of the CPO.

At the same influence on the information circulating in the process of functioning of the CPO, several processes of danger, it is necessary to consider a possibility of display of synergetic effect. In this case, the probability of exceeding the norm for two common aspects of the danger to the information circulating in the process of functioning of the CPO shall be calculated as:

$$P_{CPO_{i.j}}^{Inf.} = P_{CPO_{i.1}}^{Inf.} + P_{CPO_{i.2}}^{Inf.} - P_{CPO_{i.1}}^{Inf.} P_{CPO_{i.2}}^{Inf.}. \quad (3)$$

The assessment of the damage from exceeding the normative indicator is calculated as the amount of damage, the type of threat components for the information circulating in the process of functioning of the CPO. Total expected loss $U_{CPO}^{Inf.}$ is determined by the formula:

$$U_{CPO}^{Inf.} = \sum_{i,j} U_{CPO_{i,j}}^{Inf.}, \quad (4)$$

where $U_{CPO}^{Inf.}$ – is the mathematical expectation of the general economic damage of the CPO from processes of danger for the information circulating in the process of functioning of the CPO; $U_{CPO_{i,j}}^{Inf.}$ – is the mathematical expectation of damage of the CPO concerning the risk of the j-th aspect of the i-th process of danger for the information circulating in the process of functioning of the CPO.

Based on the material presented in the form of expressions (1)–(4) concerning the distribution of the risk-based approach to assessing the vulnerability of the CPO and based on the basic tenets of systems theory and synergetics, the level of the CPO protection in the probabilistic manifestation of various aspects of information threat of economic efficiency of functioning of system of information security of cyber protection object – F_{SISCPO}, shall be written as an equation:

$$Z_{CPO}^{Inf.} = \varphi\left(U_{CPO}^{Inf.}, F_{SISCPO}\right). \quad (5)$$

The expression (5) is presented in the form of a general functionality, the solution to which is possible while conducting the audit by experts of the situation center under security in the probable

manifestation of various aspects of the information threat process of a particular cyber protection object.

Figure 2: The main types of threats to the information circulating during the functioning of the cyber protection object [11]

4. Peculiar properties of decision support by experts of the situational center under uncertainty of the input information at emergence of threats to the information circulating in the process of functioning the cyber protection object

In general [12–14,19], the admissible set of solutions contains subsets of consistent X^S and contradictory (compromise) X^C solutions. A feature of the latter is the impossibility of improving any particular criterion $k_j(x), j = \overline{1,n}$ without deteriorating the quality of at least one particular criterion. In this case, by definition, an effective solution x° necessarily belongs to the area of compromise. This means that the problem of multiobjective optimization

$$x^\circ = \arg \underset{x \epsilon X}{\text{extr}} \langle k_j(x) \rangle, \quad \forall j = \overline{1,n} \qquad (6)$$

has no solution, i.e. is incorrect according to Adamar, since in the general case it does not provide the definition of the only optimal solution from the set of compromises X^C.

Thus, the problem of multiobjective optimization arises. The main idea of the methods for solving a multicriteria decision-making problem (MDMP) is to develop a certain regularizing procedure that allows choosing a single solution from the area of compromises X^C. There are two possible approaches to the implementation of such a task: heuristic, when the decision-maker (DM) makes a choice based on their experience, and formal, based on some formal rules (compromise schemes) [20,21].

The main methods of regularizing the problem of multicriteria optimization are the principle of the main criterion, functional-cost analysis and the principle of sequential optimization. Each of the listed optimality principles has its own area of correct application and is used in engineering practice, but the most general and universal approach is based on the formation on a set of particular criteria $K = K_\phi \cup K_з = \{k_i(x)\}, \ i = \overline{1,n}$ of a generalized scalar estimate (criterion), which is often called a utility function of the form

$$\overline{K}(x) \equiv P(x) = F\left[\lambda_j, K_j(x)\right], \ j = \overline{1,n}, \ (7)$$

where λ_j – is the isomorphism coefficients that bring heterogeneous particular criteria $K_j(x)$ to isomorphic form.

The theoretical basis for the formation of multicriteria scalar estimates is the utility theory, which assumes the existence of a quantitative assessment of the preference of decisions. It means that

$$x_1, x_2 \epsilon X, \ x_1 \succ x_2, \text{ then } P(x_1) > P(x_2), \ (8)$$

where $P(x_1)$, $P(x_2)$ – are the utility functions.

In the general case, the converse is also true. Thus, utility is a quantitative measure of the "quality" of decisions, therefore

$$x^\circ = \arg \max_{x \epsilon X} P(x). \qquad (9)$$

In this regard, the problem arises of substantiating the rule (metric), according to which the utility function is formed in the space of particular criteria $k_i(x)$.

It is crucial that there is no objective metric, and the principle of ranking decisions reflects the subjective preferences of a particular decision maker.

Consider the systemological grounds for choosing the metric of the utility function.

The synthesis of any mathematical model, including the synthesis of the utility function, presupposes the need to solve two interrelated problems: structural and parametric identification. The first of them provides for: identification of significant factors that affect the output of the model; structure definition, i.e. the kind of operator that determines the connection between the input and output data of the model.

The solution to the problem of parametric identification is to determine the specific quantitative values of the model parameters.

The problem of structural identification of a model is connected with the heuristic advance and verification of a hypothesis. In the case under consideration, the form of the decision utility function x is determined by particular characteristics (criteria) $k_i(x)$

The next step in solving the problem is to identify the type of operator F. There are most widely known two forms of the utility function: additive and multiplicative.

Additive utility function. Fishbern made a great contribution to substantiating this hypothesis. He determined the necessary and sufficient conditions for the adequacy of the additive utility function for many cases. In the case of n factors, the condition for the additivity of the utility function according to Fishbern can be formulated as follows: the factors $x_1, x_2, \dots, x_n$ are additively independent if the preference of lotteries on $x_1, x_2, \dots, x_n$ depend only on their marginal probability distributions.

Using this definition, we can formulate the main result of the theory of additive utility:

$$P(x) = \sum_{i=1}^{n} \lambda_i k_i(x). \quad (10)$$

The multiplicative form of the utility function has the following form

$$P(x) = \prod_{i=1}^{n} \lambda_i k_i(x). \quad (11)$$

The analysis showed that the multiplicative form does not allow considering the information about the weight coefficients. The disadvantage of the additive form is that it does not allow considering the nonlinearity and interconnection of particular criteria.

Therefore, in the general case, a more universal structure of the utility function is needed, which would allow considering both the additive form and nonlinear effects.

As such a universal form, the Kolmohorov-Habor polynomial can be used, which in the general case has the form:

$$\begin{gathered} P(Y) = \lambda_0 + \sum_{i=1}^{n} \lambda_i x_i + \\ + \sum_{i=1}^{n} \sum_{i \le j} \lambda_{ij} x_i x_j + \\ + \sum_{i=1}^{n} \sum_{i \le j} \sum_{k \le j} \lambda_{ijk} x_i x_j x_k + \cdots, \end{gathered} \quad (12)$$

For the purposes of evaluating utility, it shall be modified by putting $\lambda_0 = 0$, as a result, it will take the form

$$P(Y) = \sum_{i=1}^{n} \lambda_i k_i + \sum_{i=1}^{n} \sum_{j=1}^{n} \lambda_{ij} k_i k_j + \ldots \quad (13)$$

Moreover, in most practical situations, it is sufficient to consider only the members of the second order.

The Kolmohorov-Habor polynomial contains the fragments of the additive and multiplicative functions and is linear in parameters. Considering that, by expanding the space of variables by introducing additional variables such as $\sum_{i=1}^{n} \sum_{j=1}^{n} k_i k_j = z_l$, we obtain an additive function of the following form

$$P(x) = \sum_{l=1}^{L} \lambda_i z_l, \quad (14)$$

Based on the above mentioned, we will consider the additive form in more detail, using model (10) for clarity. All particular criteria, by definition, have different dimensions, intervals and measurement scales, i.e. are not comparable to each other.

Consequently, formula (9) is valid only if λ_i considers the importance of particular criteria and, at the same time, are the isomorphism coefficients, i.e. lead heterogeneous $k_i(x)$ to a single dimension and range of change. However, in the general case, it is difficult to determine the values of such isomorphism coefficients. This circumstance can be overcome by presenting the additive utility function in the following form:

$$P(x) = \sum_{i=1}^{n} a_i k_i^{\text{н}}(x), \quad (15)$$

where a_i – is the relative dimensionless weight coefficients for which the constraints are satisfied

$$0 \le a_i \le 1, \ \ \sum_{i=1}^{n} a_i = 1, \quad (16)$$

and $k_i^{\text{н}}(x)$ – normalized, i.e. partial criteria reduced to isomorphic form. The criteria are normalized according to the formula

$$k_i^{\text{н}}(x) = \left(\frac{k_i(x) - k_i^{\text{нх}}}{k_i^{\text{нл}} - k_i^{\text{нх}}} \right)^{\alpha_{\text{ш}}} \quad (17)$$

where $k_i(x)$ – is the value of a particular criterion; $k_i^{\text{нл}}$, $k_i^{\text{нх}}$ – respectively, the best and worst value of the particular criterion, which he takes on the area of admissible solutions $x \in X$.

Depending on the type of extremum (direction of dominance)

$$k_i^{\text{нл}} = \begin{cases} \max\limits_{x \in X} k_i(x), if k_i(x) \to max \\ \min\limits_{x \in X} k_i(x), if k_i(x) \to min \end{cases} \quad (18)$$

$$k_i^{\text{нх}} = \begin{cases} \min\limits_{x \in X} k_i(x), if k_i(x) \to max \\ \max\limits_{x \in X} k_i(x), if k_i(x) \to min \end{cases} \quad (19)$$

The estimation model (15) is constructive only if the weighting coefficients a_i of particular criteria are set by point quantitative values. As it was mentioned above, decision makers are the carriers of this information, which means that some procedures for obtaining it are necessary, i.e. solving the problem of parametric identification of the model. For various reasons, to obtain accurate quantitative information about the values a_i is not always possible, therefore, in the general case, the evaluation of the usefulness of decisions has to be carried out under conditions of a greater or lesser degree of uncertainty about the mutual importance of particular criteria. In general, the general model for determining the utility of a solution $x \in X$ has a form

$$P(x) = G[J(a_i), k_i(x)], i = \overline{1,n}, \quad (20)$$

where $J(a_i)$ – is the information about the values of the coefficients of relative importance.

Extreme situations are ones when:

1) the weight coefficients a_i are specified in the form of exact point quantitative values;

2) information about the preference of particular criteria is completely absent.

Typically, between these extremes, there are many situations with varying degrees of uncertainty in the assignment of weighting factors.

Based on the presented approach, the problem of synthesizing a model for calculating the interval phased value of a scalar multifactorial assessment of the effectiveness (utility) of feasible solutions is solved in this study.

It is assumed that the model for calculating the utility function in the general case is a certain fragment of the Kolmohorov-Habor polynomial, linear in parameters, but nonlinear in variables (partial criteria). This means that in the extended space of variables, the utility function model $P(x)$ can be viewed as an additive function of the form

$$\overline{P}(x) = \sum_{i=1}^{n} \overline{a_i}\, \overline{k_i^H}(x) \quad (21)$$

where $\overline{a_i}$ – is dimensionless weight coefficients that meet the requirements $0 \le a_i \le 1, \sum_{i=1}^{n} a_i = 1$, $\overline{k_i^H}(x)$ are normalized, that is, reduced to dimensionless form, the same metric and dominance direction, partial criteria; the "-" sign means interval uncertainty.

An analysis of the features of the problem of multicriteria scalar estimates showed that fuzzy sets are a widespread form of representing uncertainties in model (21). Under the accepted assumptions, the parametric identification of the model of the multicriteria optimization problem (21) consists in determining the interval values of the parameters $\overline{a_i}$ and particular criteria $\overline{k_i}(x)$, their fuzzification and calculating the interval phased value of the solution utility function $P(x)$.

Since the problem of multivariate estimation is an intellectual procedure and there are experts who are carriers of the input information, the problem of parametric identification of model parameters (21) is solved directly by the methods of expert assessment or by the method of comparative identification.

The method of comparative identification of the additive model for scalar evaluation of the utility of alternatives is as follows. The input information is the relation of a strict or non-strict order, determined by experts on a set of admissible alternatives

$$x_1 \succ x_2 \sim x_3 \sim x_4 \succ \cdots, \quad (22)$$

where $\succ, \sim$ are the signs of advantage and equivalence correspond. According to the theory of utility for (22), the following relations hold:

$$P(x_1) > P(x_2) = P(x_3) > P(x_4) > \cdots, (23)$$

Based on (23), one can compose a system of equations of the form

$$\begin{aligned} &P(x_2) - P(x_1) \le 0, \\ &P(x_3) - P(x_2) = 0, \\ &P(x_4) - P(x_3) \le 0. \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned} \quad (24)$$

By substituting the utility function (21) into (24), we obtain a system of a_i irregularities that are linear with respect to the parameters, which determine the area of their possible values. The method of linear programming on the selected area determines the interval values $\left[a_i^{max}, a_i^{min}\right]$ of the parameters. In this case, regardless of the method, interval estimates of the parameters are determined $a_i = \left[a_i^{max}, a_i^{min}\right], \forall i = \overline{1,n}$, and the size of the intervals depends on the scatter of the subjective individual labels of experts.

The interval uncertainty of the model variables (particular criteria) is determined by non-factors. Their analysis and accounting allows you to determine the range of possible values of each of them.

The next stage in identifying the model (21) consists in its fuzzification, that is, in the choice of the type and parameters of the membership function of the interval parameters and changes.

The weight coefficients a_i are interval fuzzy numbers, and the value of particular criteria can be specified both numerically, in the form of fuzzy numbers, and qualitatively, in the form of linguistic terms.

5. Conclusions

1. It is shown that the basis of the information security system of a cyber protection object shall

be a classical control loop that provides collection, processing and analysis of information, as well as modeling the development of information danger at a cyber protection object and the development and implementation of anti-crisis management to prevent the emergence of threats to information circulating in the process of functioning of the cyber protection object, as well as the elimination or minimization of their consequences.

2. The indicator of risk for information circulating during functioning of the cyber protection object is the sum between the indicators of risk of information disclosure and information leakage, as well as the indicator of risk for computer information circulating during functioning of the cyber protection object.

The indicator of the risk of information leakage includes indicators of the risk of information leakage through technical channels, information leakage through communication channels, speech information leakage, as well as information leakage, shown information.

The risk indicator for computer information includes indicators of the risk of loss and alteration of information, as well as obtaining unauthorized access to information.

3. It is shown that while conducting the audit by the experts of the situational center under security in conditions of probabilistic manifestation of various aspects of the information threat process of a cyber protection object, the procedure for making management decisions is complicated by the fact that the necessary conditions for the effectiveness of decisions are their timeliness, completeness and optimality. Therefore, increasing the efficiency of the decisions made is associated with the need to solve the problem of multi-criteria optimization under the uncertainty, which requires the development of formal, normative methods and models for a comprehensive solution to the problem of decision-making under the multi-criteria and uncertainty in managing the processes of preventing the occurrence of threats to information circulating during functioning of the cyber protection object, as well as elimination or minimization of their consequences.

4. In order to solve the problem of multicriteria optimization under the uncertainty, in the study, firstly, it is formalized the methods for obtaining initial information about the advantages of a decision-maker, based on both traditional heuristic procedures for expert evaluation and formal methods of comparative identification. It is shown that regardless of the method of obtaining the initial information and the form of its presentation, the most adequate is the interval assessment of the preferences of the decision-maker. Secondly, a model of a multicriteria scalar assessment of the usefulness of feasible alternative solutions has been synthesized.

5. The presented results represent the scientific basis for the development of a support system for making anti-crisis decisions in critical situations by experts of the situational center to ensure the appropriate level of information security of the cyber protection object.

6. References

[1] Basic principles of cybersecurity in Ukraine Act dated on October 5, 2017 No 2163-VIII [Electronic resource]. Access mode: https://zakon.rada.gov.ua/laws/show/2163-19

[2] Cybersecurity Strategy of Ukraine approved by the President of Ukraine Order concerning the Regulation of the National Security and Defense Council of Ukraine dated on January 27, 2016 [Electronic resource]. Access mode: https://zakon.rada.gov.ua/laws/show/96/2016

[3] General requirements for cyber protection of critical infrastructure, approved by Cabinet of Ministers of Ukraine Regulation dated on June 19, 2019 No 518

[4] V. Tiutiunyk, V. Kalugin, O. Pysklakova, A. Levterov, Ju. Zakharchenko "Development of Civil Defense Systems and Ecological Safety". IEEE Problems of Infocommunications. Science and Technology (2019): 295–299.

[5] B. Fahimnia, C.S. Tang, H. Davarzani, J. Sarkis. Quantitative models for managing supply chain risks: A review. European Journal of Operational Research, 2015, No.247, pp.1–15.

[6] S. Haugen, J.E. Vinnem. Perspectives on risk and the unforeseen. Reliability Engineering and System Safety, 2015, No.137, pp.1–5.

[7] F. Khan, S. Rathnayaka & S. Ahmed Methods and models in process safety and risk management: Past, present and future. Process Safety and Environmental Protection, 2015, No.98, pp.116–147.

[8] T. Aven. Risk assessment and risk management: Review of recent advances on their foundation. European Journal of

Operational Research, 2016, Vol.253, No.1, pp.1–13.
[9] V. Tiutiunyk, I. Ruban, O. Tiutiunyk "Cluster analysis of the regions of Ukraine by the number of the arisen emergencies". IEEE Problems of Infocommunications. Science and Technology (2020).
[10] J. Gehandler, U. Millgård. Principles and Policies for Recycling Decisions and Risk Management. Recycling, 2020, Vol.5, No.21, pp.1–18.
[11] O.Svynchuk, O. Barabash, J.Nikodem, R. Kochan, O. Laptiev. Image compression using fractal functions.Fractal and Fractional, 2021, 5(2), 31.pp.1-14
[12] Oleksandr Laptiev, Savchenko Vitalii, Serhii Yevseiev, Halyna Haidur, Sergii Gakhov, Spartak Hohoniants. The new method for detecting signals of means of covert obtaining information. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.176 –181.
[13] Ye.H. Petrov, N.A. Brynza, L.V. Kolesnik, O.A. Pysklakova. Methods and models of decision making under the multi-criteria and uncertainty. Kherson, 2014.
[14] S. Toliupa, N. Lukova-Chuiko, O. Oksiuk. Choice of Reasonable Variant of Signal and Code Constructions for Multirays Radio Channels. Second International Scientific-Practical Conference Problems of Infocommunications. Science and Technology. IEEE PIC S&T 2015. pp. 269 – 271.
[15] N. Lukova-Chuiko., I. Ruban, V. Martovytskyi. Approach to Classifying the State of a Network Based on Statistical Parameters for Detecting Anomalies in the Information Structure of a Computing System.Cybernetics and Systems Analysis.Vol. 54. № 2. 2018. pp. 142 – 150.
[16] N. Lukova-Chuiko, V. Saiko, V. Nakonechnyi, T. Narytnyk, M. Brailovskyi. Terahertz Range Interconnecting Line For LEO-System. 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine. 2020. pp. 425– 429.
[17] A.O. Korchenko, V.O. Breslavskyi, S.P Yevseiev, N.K. Zhumangalieva, A.O. Zvarych, S.V. Kazmirchuk, O.A. Kurchenko, O.A. Laptiev, O. V. Severinov, S. S. Tkachuk. Development of a method for construction of linguistic standards for multicriterial evaluation of HONEYPOT efficiency. Eastern-European journal of enterprise technologies. Vol.1№2 (109), 2021 pp. 14–23. ISSN (print)1729 - 3774. ISSN (on-line) 1729-4061.
[18] Mashkov V.A. and Barabash O.V. Self-Testing of Multimodule Systems Based on Optimal Check-Connection Structures. Engineering Simulation. Amsterdam: OPA, 1996. Vol. 13, pp. 479 – 492.
[19] Oleg Barabash, Andrii Musienko, Spartak Hohoniants, Oleksandr Laptiev, Oleg Salash, Yevgen Rudenko, Alla Klochko. Comprehensive Methods of Evaluation of Efficiency of Distance Learning System Functioning. International Journal of Computer Network and Information Security(IJCNIS), Vol. 13, No. 1, Feb. 2021. pp 16–28.
[20] V. Sobchuk, V. Pichkur, O. Barabash, O. Laptiev, K. Igor and A. Zidan, Algorithm of Control of Functionally Stable Manufacturing Processes of Enterprises. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2020, pp. 206-210, doi: 10.1109/ATIT50783.2020.9349332.
[21] Maksymuk O., Sobchuk V., Salanda I., SachukYu. A system of indicators and criteria for evaluation of the level of functional stability of information heterogenic networks. / // Mathematical Modeling and Computing. – 2020. – Vol. 7, No. 2. – pp. 285 – 292