INFORMATION RISK MANAGEMENT BASED ON FUZZY COGNITIVE MODELING

Salahaddin Yusifov, Imran Bayramov, Aygun Safarova,
Elchin Melikov, Tamella Magerramova

Azerbaijan State Oil and Industry University
siyusifov@mail.ru
imranb1963@mail.ru
aygsafa@rambler.ru

Abstract

The article examines information risk management using fuzzy cognitive modelling. Within the framework of the FCM methodology, a graph was constructed to identify the cause-and-effect relationships between the main concepts in the subject area that give rise to risk, in order to assess current risk levels. A method for determining an acceptable level of risk under subjective uncertainty, based on expert information, was developed. To determine the acceptable risk level for an organisation, the functional dependence of the probability of loss on its scale was established, and a graph of this dependence was created. To more fully reflect the decision-maker's opinion on the volume of acceptable risk, the concept of an acceptable risk curve was applied. This allows both numerical and verbal expert assessments to be taken into account, reducing the level of subjective uncertainty. An algorithm for constructing this curve was also developed.

Keywords: Fuzzy cognitive model, acceptable risk zone, information security, linguistic variable, polygon of possible risk values, tolerant risk zone

I. Introduction

Any activity, except for material and energy flows, necessarily contains an information component. At the same time, in ensuring the reliable functioning of information processing processes and achieving the required level of information security, the management of risks of violation of information properties (confidentiality, availability, integrity, etc.) in the process of its processing (information risk management) plays a special role. The problem of information risk management is a complex task that combines a number of different areas: the preparation of an agreed opinion on the acceptable level of risk; assessment of the current state of risks in the coordinate space "harm from threats - probability of realization of the danger"; finding acceptable measures for the decision-maker to reduce the risk level to target values; implementation of the solutions found. At the same time, most of the parameters used in the process of preparing management decisions do not have crisp (numerical) values, are formulated by experts in verbal form and are subjective. In addition, there is an ambiguity of the concept of "risk", as well as opportunities to eliminate various manifestations of risk and its negative consequences. Thus, the assessment and management of risks arising in the information processing process is a complex, poorly structured, and poorly formulated type of activity.

II. Problem solving methods

Risk management includes risk analysis (assessment), development and implementation of management decisions. Risk analysis involves identifying vulnerabilities and threats, assessing possible impact, which allows choosing adequate protective measures for those systems and processes in which they are needed. It helps the company rank the list of risks, determine and justify the reasonable cost of protective measures and make the security of the functioning of information systems cost-effective, relevant, timely and capable of responding to threats.

1. Algorithm for determining acceptable risk based on expert information

One of the basic, or "central" concepts of the risk management process is the concept of acceptable risk. Acceptable risk is understood as the risk that a decision-maker is willing to accept in a given situation [8].

In the mathematical formulation of the problem, the risk quantity is usually calculated using the following formula:

$$R = P \otimes U,$$

so, here P is the probability of an unfavorable event occurring;
U is its consequences;
$\otimes$ – is a composition that is determined in a certain sense .

However, the prices obtained in this way are not sufficiently informative for the decision-maker and do not allow him to make informed choices in management decisions.

Therefore, another approach is needed to assess acceptable risk, which is based on the following assumption: the greater the potential harm, the lower the probability of its occurrence must be for the decision-maker to be willing to accept it. Thus, the essence of the concept of "acceptable risk" can be written as follows:

$$\forall U \exists ! P : P^*(U) = P \quad (1)$$

Based on this, it is generally proposed to consider the functional dependence of the probability of a certain loss occurring on its quantity, which is described by the acceptable risk curve:

$$P^* = P^*(U), \quad (2)$$

so that here $P^*(U)$ is a monotonically decreasing function reflecting the acceptable probability $U^{\min or}$ of the occurrence of damage ; $U^*: U^* \in [U^{min\,or}; U^{crtic}]$- is the damage that is insignificant for the decision maker, that is, the value below which damage is not taken into account; U^{critic} - critical, that is, is the maximum acceptable damage for the decision maker, since the probability of its occurrence should be minimal and ideally tends to zero.

P(U)* can be varied. For example, the probabilities of possible losses in accidents are often described by a Gaussian distribution [18; 118]. In some cases, $P^* = a/(1+\exp(b \cdot (U - U^{\min or}))$ it is appropriate to use a function that describes an S-shaped curve.

P^* The following function can be used as a quantity:

$$P^* = a \cdot \exp(b \cdot (U - U^{\min or})), \quad (3)$$

so that here: the constant a $U^{\min or}$ corresponds to the probability of minimal "insignificant" damage occurring; the constant b U^{critic} determines the rate of decrease in the acceptable probability of accepting damage as it approaches its value.

The choice of the exponential function for the approximation is due to its widespread use in describing experimental data in various fields. In particular, the exponential function provides a good approximation of the piecewise linear Farmer function, which is widely used in assessing the risks associated with man-made accidents and natural disasters [11;12].

Formation of an expert group

The following should be considered when establishing an expert group to determine the acceptable risk quantity and selecting experts to be included in it:

- experts should be selected from among managers;
- experts should be selected from departments that ensure reliable operation of the information processing process;
- experts should be selected from departments dealing with the economic (financial) support of the organization's activities;
- certain external experts should be selected by agreement.

It is also necessary to include experts who are familiar with the organization's activities and have qualifications and experience in the field of information technology application and (or) information security, as well as in the field of economics and enterprise management.

The independence of the experts is one of the most important issues. There should be no factors (commercial and financial interests or other pressures) that could influence the decisions they make. Thus, the composition of the expert group should consist of at least four experts.

The Delphi method can be used to coordinate the opinions of experts [9; 10].

Algorithm for constructing an acceptable risk curve

classify the amount of potential damage to an organization's assets as a result of an adverse event ( ). While verbal forms are used to describe categories of damage, the Harrington scale is used to compare numerical values for different damage classes [96]: “Negative damage” - 0.1·U U_i^{critic}; "Slightly significant damage" - 0.29·U^{critic}; "Moderate damage" - 0.51·U^{critic}; "Significant damage" - 0.72·U^{critic}; "Critical damage" - 1·U^{critic}.

2) The decision maker U_i assesses the probabilities of occurrence $R^* = \{(U_i; P_i^*)\}_{i=\overline{1,N}}$ of various categories of harm : P_i^* in terms of their acceptability.

3) The values U_i indicated at the reference points P_i^* are approximated by the continuous function in expression (3) using the least squares method. As a result of the approximation, the values of the coefficients ***a*** and ***b*** are found.

A graphical representation of the acceptable risk function is depicted below (Fig. 1).

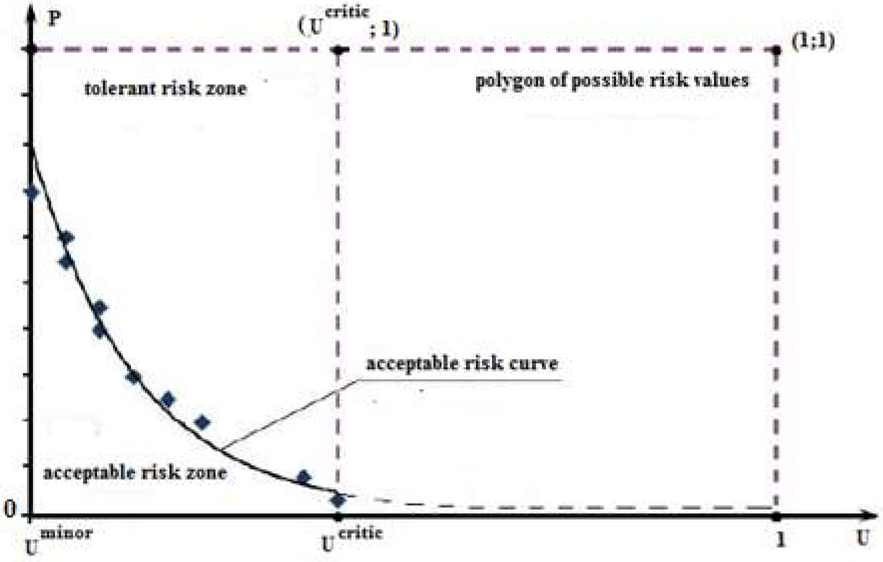

Figure 1: *Graph of the acceptable risk function*

Along with acceptable risk, the concept of tolerable risk is also used in risk management, that is, the maximum level of risk that an organization can tolerate without significant damage to its financial and competitive position [9;6]. Typically, the tolerable risk level is defined as a share of the company's authorized capital and is determined by the internal risk management policy. In Figure 1, this concept corresponds to the tolerable risk zone located on the border of the rectangle with vertices (U^{minor}; 0), (0; 1), ($U^{critical}$; 1), ($U^{critical}$; 0). The rectangle with vertices (U^{minor}; 0), (0; 1), (1; 1), (1; 0) is called the polygon of possible risk values. The area bounded by the coordinate axes and the acceptable risk curve constitutes the acceptable risk zone.

In the case of a discontinuous P* function, the acceptable risk quantity is found using the following formula:

$$R^{accep} = \left[\int_{U^{\min or}}^{U^{critic}} P^*(U)dU \right] / \left(U^{critic} - U^{\min or} \right). \quad (4)$$

In formula (4), the denominator represents the area of the tolerant risk zone. Dividing the tolerant risk zones into areas allows us to normalize the risk level with respect to the critical value.

2. Building a fuzzy cognitive model for assessing current (relevant) risks of information processing

The fuzzy cognitive model (FCM) methodology involves constructing a fuzzy cognitive graph that reflects the relationship between the main factors of the subject area and their mutual influence; assessing the state of factors and the degree of their influence on other concepts in the hierarchy; and calculating the values of concepts above the hierarchy based on the known values of the factors affecting them. Let's consider each of these stages.

2.1. Construction of a fuzzy cognitive graph

A fuzzy cognitive model for assessing current and relevant risks of information processing can be described as an 8-level graph as follows (Fig. 2).

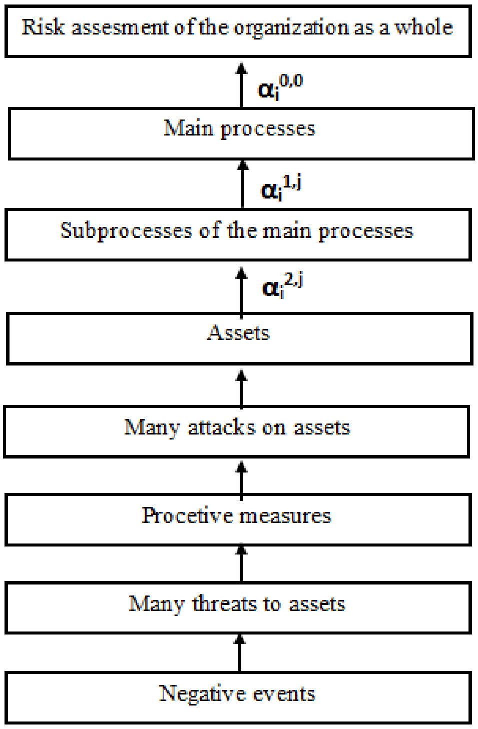

Figure 2: *Levels of the FCM graph for assessing current risks*

Let's denote the described graph by G and explain it level by level:

At the lower, 7th level, there are concepts that reflect the probability of a negative event that could pose a threat to the information assets involved in the organization's core business processes. In general, each negative event can pose many threats of varying intensities with varying probabilities, which in turn determines the level of possible damage to the organization's information assets.

Therefore, at level 6, I_i concepts are located that reflect the intensity and probability of occurrence of possible threats caused by negative events of level 7. In this case, intensity is understood as the potential harm that a threat can cause. P_{I_i}

At level 5 I_i, concepts $Z_{P_{I_i}}$ reflecting the effectiveness of the protection measures applied to reduce their quantity Z_{I_i} and quality P_{I_i} are located.

At level 4, there are concepts that correspond to the probability and degree of destructiveness (carried out despite the implementation of security measures and threats) of attacks on information assets supporting the organization's sub-processes.

At Level 3 risks to assets reflect the likely deterioration of the condition of the organization's information assets.

At Level 2 concepts reflect risks to sub-processes of the organization's core processes and describe the decomposition of level 1 concepts. The decomposition is carried out until it is possible to identify all significant information assets that may be subject to attacks.

At Level 1 includes concepts that reflect risks to the organization's core processes (i.e., the likely reduction in the quality of the execution of a key event).

At Level zero includes an assessment of the information processing risks of the organization as a whole and a corresponding overall (integrated) risk assessment.

The values of some concepts included in the graph hierarchy can be determined numerically. For example, after processing the collected statistical data, numerical data are obtained. However, in most cases, it is difficult to determine the values of factors numerically, and therefore it is necessary to resort to expert assessment methods. Expert assessments are usually verbal in nature. Therefore, to formalize the information received from the expert , it is necessary to include a linguistic variable *L, the values of which are a set of terms:*

QL = {Low (A); Below Average (OA); Average. (O); Above Average (OY); High (Y)}. (5)

To move on to quantitative description, it is appropriate to associate this term set with a five-level classifier, where the membership functions of fuzzy numbers describe a trapezoid given in the segment [0; 1]:

{ "A" (0; 0; 0.15; 0.25); "OA" (0.15; 0.25; 0.35; 0.45); "O" (0.35; 0.45; 0.55; 0.65);
"OY" (0.55; 0.65; 0.75; 0.85); "Y" (0.75; 0.85; 1; 1)}, (6)

Using a classifier allows you to move from a qualitative (verbal) description of a parameter to a quantitative description in the form of a corresponding membership function of fuzzy trapezoidal numbers.

If, in addition to qualitatively assessed factors (“fuzzy”), FCM contains concepts whose values are quantitatively determined crisp , then it is appropriate to use the proposed method for the joint use of quantitative and qualitative information [4]. Thus, the following formula is used to calculate the quantitatively measured *F i* It involves calculating the normalized value according to the factor . $\overline{F_i}$

$$\overline{F_i} = (F_i - F_{\min}) / (F_{\max} - F_{\min}), \tag{7}$$

where *F max* and *F min* are the maximum and minimum values of *F i* , respectively .

is described by $(a_1 = a_2 = a_3 = a_4 = \overline{P_i})$ a fuzzy number X such that (a_1, a_2, a_3, a_4). If has $\overline{P_i}$ a quantity δ error, then $a_1 = a_2 - \delta; a_2 = a_3 = \overline{P_i}; a_4 = a_3 + \delta$. Thus, the normalized crisp value of the factor is described as a special case of a fuzzy in the interval [0;1].

To take into account the interaction of concepts in a cognitive graph, $\{\alpha_{ij}\}$ it is necessary to consider the set of weights of the edges of this graph.

2.2. Determination of the intensity of interaction of factors

$\{\alpha_{ij}\}$ The values of the weights from the set (usually, $\alpha_{ij} \in [-1;1]$) can be obtained by interviewing experts. For example, in the Situation and Compass systems, the expert compiles a set of linguistic assessments reflecting the strength of the influence. Then, each element of the set of assessments is depicted as equidistant points on the [–1; 1] partition [6].

The Canvas system uses indirect methods to determine the strength of the impact: the expert estimates the possible change in the impact factor values for a given change in the result factor value. According to the authors, this should help reduce the error in the expert assessment [6].

These approaches involve moving the maximum price from the lower to the upper level of the FCM, and this is based on the assumption of the independent influence of causes on the influencing factors.

If the value of the increase in the resulting factor is related to the combined effect of several factors, then the contribution of each causal factor must be determined differently. Such models were proposed by Roberts and later analyzed in the works [5;12].

At this point, "it should be noted that "soft" quality measurements such as comparison, class assignment, ordering are much more reliable than subjective probabilities, quantitative assessments of the importance of criteria, "weights" of utilities, etc." [2; 7]. In addition, in most cases, experts have difficulty in providing accurate numerical assessments. As a result, it is preferable to use ranking methods whose application requires only the ranking of factors.

In [4], a modification of the non-rigorous ranking method was proposed to assess the intensity of fuzzy relationships between factors. According to this, the expert numbers all the criteria in increasing order of importance. Sometimes, cases are also allowed when the expert cannot distinguish some criteria from each other. In this case, during the ranking, the expert puts them in the same position in an arbitrary order. Then the positions of the sorted list are numbered sequentially. The rank of the factor is determined by its number. If several factors that do not differ from each other are in the same position, then the number of its group in the ranking is taken as the rank of each of them. The values found by this method are a generalization of the concept of Fishburne weights to the situation where, in addition to preferences, there are also indifference relations.

When using this method, it is necessary to determine the dominance relations in the graph *G :*

$$E = \{GF_i(e)GF_j \mid e \in (>, \approx)\}, \tag{8}$$

here GF_i and GF_j Factors located at the same level of the hierarchy; $\approx$ *indifferent* attitude; > It is a relationship of superiority.

allows us to determine normalized Fishburne weights (connection weights) for the arcs of the graph GD_{ij} *G* for the case of the joint influence of several causal factors on the effect factor.

When determining the "weights" of the main business processes, their contribution to the organization's activities (for example, the share of profit attributable to the main process) is taken into account. Thus, the "weights" of the main process and sub-processes are normalized by the number 1. In turn, the weight coefficients of information assets in the sub-process are defined as the sensitivity of the sub-process to the failure of this asset and can take values from 0 to 1.

2.3. Calculation and defuzzification of fuzzy values of fuzzy cognitive model concepts

In FCM , to calculate the values of concepts, it is necessary to linguistically estimate the values of the parameters of the lower levels of the hierarchy (using the values of the QL term-set) and determine the set of influence weights *{α_{ij}}* . Then, the influences of the concepts located lower in the hierarchy are aggregated according to the rules ***R*** *$_i$*, so in this case, additive, multiplicative, minimax, etc. curves of the vector criterion can be used. In this case, if it is possible to compensate for the values of some factors by others, an additive curve can be used. Unlike an additive curve, the value of a multiplicative curve decreases sharply with a decrease in the individual individual scores. This allows us to take into account such options when making decisions, when each of the factors is significant and there is no mutual compensation between them. In especially critical cases, it is necessary to use extreme (minimum or maximum) values (the "weakest link" principle). In this case, it is appropriate to use the centroid method to compare trapezoidal fuzzy numbers, since the calculation of "average" values most fully reflects the characteristics of this type of fuzzy numbers [4].

When assessing the risks arising from the combined effects of a finite number of independent hazards, the following additive equation can be used:

$$F = \sum_i \alpha_i F_i , \tag{9}$$

where are the weights of the influence of α_i the quantity F_i factors on the F factor.

In this case $\alpha_i \in [0;1]$, when finding the svyortkas, the values of some concepts must first be inverted to take into account their negative effect. To find the inverse value (inversion) of the linguistically described factor *F*, the following formula can be used:

$$Inv(F) = (1 - \mu(F)), \tag{10}$$

Here $\mu(F)$ F is the membership function of the fuzzy number corresponding to the linguistic value of the factor.

When finding the svortkas, the product or sum of linguistic values is understood as the product or sum of the corresponding fuzzy numbers. It is also possible to use special software for calculations with fuzzy numbers .

The result of operations with fuzzy numbers is also a fuzzy number that must be defuzzified in order to make a judgment about the quantitative level of indicators. The "center of gravity" method can be used to defuzzify the calculated fuzzy value. When choosing trapezoidal fuzzy numbers of type (6) as a classifier, the defuzzification function (Def) of an arbitrary trapezoidal fuzzy number A will have the following form:

$$De(A) = (a_2 + a_3) / 2 . \tag{11}$$

For example, a verbal score of "above average" (OY) corresponds to a trapezoidal number (0.55; 0.65; 0.75; 0.85). Its fluency is (0.65+0.75)/2= 0.7.

The resulting defuzzified value is a metric characteristic that reflects the state of the concept in the FCM.

The following tuple can be used as a fuzzy cognitive graph to assess the current risks of information processing :

$$RSK =< G, QL, \{\alpha_{ij}\}, R, Def >, \tag{12}$$

where G is a fuzzy cognitive graph reflecting the relationship of the main concepts involved in risk assessment; QL is the term-set of linguistic evaluations of parameter values (2.5) with the corresponding fuzzy classifier (2.6); $\{\alpha_{ij}\}$ is the set of weights of the languages of the graph G to find which preference relations are determined on the graph, which in turn allows us to determine normalized Fishburne weights (relationship weights) for the arcs of the graph G using the non-strict ranking method; R is a set of rules that aggregate the influence of various lower-level concepts on the higher-level concept; Def is the fuzzy value defuzzification function obtained as a result of calculations using the fuzzy cognitive graph.

If it is necessary to include new knowledge obtained as a result of studying the processes affecting the risk level in a specific system in the proposed model, it is advisable to present this knowledge as a low-level fuzzy cognitive model built according to the scheme described above. This method of hierarchically constructing fuzzy models allows for the unification of the description of knowledge and contributes to its more efficient storage and processing.

In general, the values of fuzzy cognitive model concepts depend on time t . Thus, when assessing risks at t = 0, it is necessary to give the initial values of the factors. Then, to find the values of the concept *Kj* for discrete values of *t = 1, 2, 3, ...,* the following formula can be used:

$$K_j(t+1) = K(t) + H(\Delta K_i, RSK, t+1)\,, \tag{13}$$

where ΔK_i - are the increments of the concepts K_j affecting K_i -; - is the generalized function of the impact $H(\Delta K_i, RSK, t+1)$ on the output price ΔK_i determined by the RSK tuple K_j .

Threats I_i intensity and their P_{I_i} The apparatus used to find values reflecting the probability of occurrence depends on the sources of occurrence of negative events at the initial moment in time.

When the threat to information assets is associated with objective processes of a technogenic or natural nature, probability theory and mathematical statistical methods can be used. As a result of their application, the threat P_{I_i} The probability of occurrence is determined and, after normalization, the intensity of each threat I_i is evaluated by the corresponding membership function in [0;1]. In this case, the number 1 corresponds to the intensity of the threat that leads to the complete destruction of the concept to which this threat is directed.

If the threat is associated with a subjective factor, then it is necessary to build a separate low-level FCM, that is, a "subject model". In this case, depending on the degree of loyalty of the subject, the goals he sets, etc., it is necessary to take into account the level of motivation for his actions, the level of his psychological and physical capabilities, his competence (level of knowledge and skills) and technical equipment, that is, the means and methods he uses, the level of his rights in relation to the assets of the system, etc.

If the probability assessment is carried out by experts and expressed verbally, then it is necessary to use the Harrington scale to convert this assessment into a numerical format [98]:

"Low probability" – 0.1; "Below average probability" – 0.29; "Average probability" – 0.51;
"Above average probability" – 0.72; "High probability" – 0.98. (14)

The probability of attacks and their destructiveness, i.e., damage to assets, during threats that occur despite the implementation of protective measures are determined by the following formulas:

$$U_{Att_i} = I_i \cdot Inv(Z_{I_i})\,, \tag{15}$$

$$P_{Att_i} = P_{I_i} \cdot Inv(Z_{P_{I_i}})\,, \tag{16}$$

where U_{Att_i} - is the level of residual damage after the implementation of the I_i *i -th attack after the protective measure;* - is the intensity of the *i - th threat* before the protective measure ; Z_{I_i} its quantity is the effectiveness of the protective measure in reducing the intensity of the i-th threat and is calculated using the formula *Inv(Z Ii)* (10); P_{Att_i} - is the residual probability of the i-th attack after the protective measure; - is the probability of the P_{I_i} *i* -th threat before the protective measure ; $Z_{P_{I_i}}$ its quantity is the effectiveness of the protective measure in reducing the probability of the i-th threat and $Inv(Z_{P_{I_i}})$ is calculated using the formula (10).

As mentioned above, one negative event can create a number of threats with different intensities and probabilities of their occurrence. This can lead to a situation where the same value of possible damage corresponds to different probabilities. The values calculated using formulas (15) and (16) U_{Att_i} reflect P_{Att_i} the risks for information assets (the third level of the FCM and allow us to consistently find the risk values for subprocesses (the second level), the main process (the first level of the hierarchy) and the organization as a whole (the zero level of the FCM.

The cost of damage at levels {0;1;2} of the graph G is calculated using the following formula:

$$U_i^{k,j} = \alpha_i^{k,j} U_i^{k+1,j}\,, \tag{17}$$

where $U_i^{k,j}$ the quantity is the i-th loss of the j-th concept of the k-th level of the QMS; $\alpha_i^{k,j}$ - is the weight coefficient reflecting the impact of the i-th loss of the (k+1)-th level concept on the j-th concept of the k-th level of the QMS; $U_i^{k+1,j}$ – is the loss affecting the j-th concept of the k-th level brought to the i-th concept of the (k+1)-th level of the QMS; $k \in \{0;1;2\}$.

When k = 2, $U_i^{2,j}$ the values of - reflect the degree of damage to the subprocess, $\alpha_i^{2,j}$ - is the weight of the i-th information asset when supporting the activity of the j-th subprocess. This coefficient is expressed verbally and is estimated using the Harrington scale; $U_i^{3,j}$ - is the amount of damage to the information asset after the threats have passed the protection measure.

When k = 1, $U_i^{1,j}$ the values correspond to the quality reduction levels of the main process, $\alpha_i^{1,j}$ is the weight of the *i -th subprocess* in the execution of the *j -th main process* .

When k = 0, $U_i^{0,0}$ their value reflects the i-th loss to the organization as a whole, $\alpha_i^{0,0}$ the share of the i-th main process in the organization's activities.

remain equal to the probabilities of attacks calculated at level 4 of the FCM . P_{Att_i}

a set of points $i = \overline{1, N}$ characterizing the current indicators of risks arising in the information processing process for the organization as a whole is obtained, where $R^{cur} = \{(U_i; P_i)\}$, so N - is the amount of possible loss values. The total value of the current risk is found by the following formula:

$$R^{cur} = \left[\sum_{i=1}^{N} (\Delta U_i \cdot P_i) \right] / U^{critic} - U^{\min or}), \tag{18}$$

where $\Delta U_i = U_i - U_{i+1}$; R^{cur} points are arranged with increasing damage value; $U_0 = U^{\min or}$.

The results of the current risk assessment can be depicted graphically as shown in the figure below (Fig. 3). The diamonds in the figure represent the reference points for constructing the acceptable risk curve, and the squares represent the points characterizing the current risks.

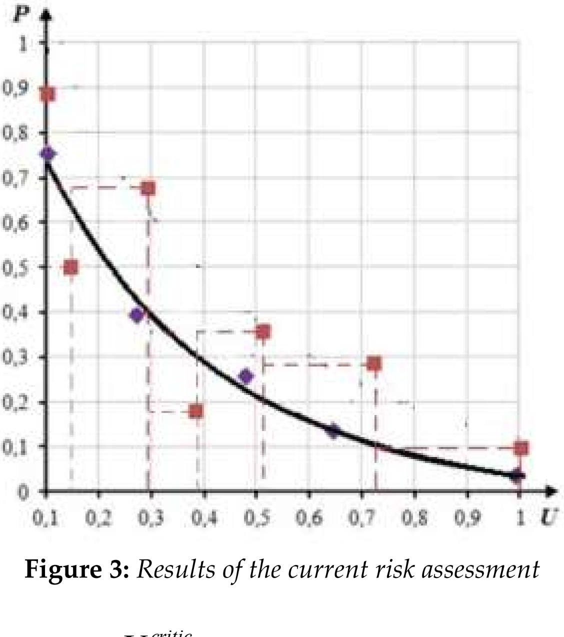

Figure 3: *Results of the current risk assessment*

Note: Damage values in Fig. 3 U^{critic} are normalized.

Thus, the following algorithm can be formulated to assess the current (actual) risks of information processing:

Stage 1. Formation of the risk assessment QMS:

1.1. Identification of the organization's key business processes.

1.2. Separation of sub-processes from the main process (if necessary).

1.3. Identification of information assets that support the activities of the subprocess.

Stage 2 – Risk Calculation:

2.1. Identification of the potential range of possible negative events and assessment of their probability of occurrence.

2.2. Identification of threats that may arise as a result of the identified negative event. Assessment of I_i the intensity of these threats and P_{I_i} the probability of their occurrence.

on the intensity and probability of $Z_{P_{I_i}}$ the occurrence of the hazard Z_{I_i} .

2.4. Calculation of the residual probabilities of attacks on information assets and indicators of damage from them after protective measures, based on formulas (15) and (16), respectively.

2.5. Calculation of the damage, i.e. the degree of damage to the subprocess by attacks, for each subprocess based on the values obtained in step 2.4 using formula (17) for k = 2.

2.6. Determining the damage to key business processes using formula (17) for k = 1. In this case, the attack probabilities calculated in step 2.4 remain unchanged in steps 2.5 and 2.6.

2.7. Calculation of information risks using formula (17) when k = 0 for the organization as a whole.

As a result of the risk assessment, a set of points is obtained that characterize the current indicators of information processing risks for the organization as a whole. In this case, if some information assets participate in more than one main process, the risks for information assets are reconsidered taking into account their weight in the main process. In this case, each such threat on the coordinate plane “harm - probability” corresponds to more than one point.

The total value of the current risk is found by formula (18). In this case, dividing the tolerant risk zone into areas and then obtaining the current values allows classifying the degree of danger of current risks during verbal assessment according to the Harrington scale.

III. Conclusion

The use of a fuzzy cognitive approach allowed the formation of a fuzzy cognitive model for assessing current information processing risks, including information security risks, selected by generalizing information about business processes carried out in the organization. The information assets supporting them were identified. Possible threats and measures to neutralize them, as well as negative situations that could pose a threat to the organization's information assets, were formed. Thus, the use of the proposed model allows determining the set of points on the "harm-probability" coordinate plane, which characterizes the current level of information risks.

CONFLICT OF INTEREST.
Authors declare that they do not have any conflict of interest.

References

[1] Azhmukhamedov, I. M. Analysis and management of complex security based on cognitive modeling. // Management of large systems. 2010. No. 29. pp. 5-15.

[2.] Asanov, A. A. Influence of reliability of human information on the results of application of decision-making methods. // Automation and Telemetry. 1999. No. 5. pp. 20-31.

[3] Vladimirov, V. L. Risk management: Risk. Sustainable development. Synergetics. Moscow: Science, 2000. 431p.

[4] Vorontsov, Ya. A. Methods of parameterized comparison of fuzzy triangular and trapezoid numbers. // Bulletin of Voronezh State University. Series: Systems analysis and information technologies, 2014. No. 2. pp. 90-97.

[5] Kornoushenko, E. K. Managing a situation using the structural properties of its cognitive map. / Proceedings of the IPU RAS. Vol. XI. Moscow: IPU RAS, 2000. pp. 85–90.

[6] Kulinich, A. A. Cognitive decision support system "Canvas". Software products and systems. 2002. No. 3. pp. 25–28.

[7] Larichev, O. I. Qualitative methods of decision making. Verbal analysis of the decision. Moscow: Nauka, 2006. 208p.

[8] Acceptable risk as a level of production safety [Electronic resource] – Access mode: http://studme.org/12810419/bzhd/priemlemyy_ risk_kak_uroven_ bezopasnosti_proizvodstva

[9] Brady, S. R. Utilizing and adapting the Delphi Method for use in qualitative research [Electronic resource] // International Journal of Qualitative Methods. 2015. vol. 14, no. 5.: http://ijq.sagepub.com/content/14/5/1609406915621381 – DOI: 10.1177/1609406915621381

[10] Hsu, C.-C. The Delphi technique: making sense of consensus / C.-C. Hsu, B. A. Sandford // Practical assessment, research & evaluation. 2007. V. 12, No. 10: http://pareonline.net/getvn.asp?v=12&n=10

[11] Stojanovski, P. Comprehensive disaster risk modeling for agriculture [Electronic resource] Planet@Risk. – 2015. – Vol. 3, No. 1: https://planet-risk.org/index.php/pr/article/view/ 166/347 .

[12] Farzalizada Z.I., Ismayilova H.G., Damirova J.R., Alakbarov, M.E., Shahlarli M.E. Fuzzy assessment of technological risks in the main oil pipeline. / WCIS 2020: 11th World Conference "Intelligent System for Industrial Automation" (WCIS-2020) AISC 1323, pp. 127-131, 2021, https://doi.org/10.1007/978-3-030-68004-6_16