Analysis and Management of Information Risks on the Basis of Fuzzy Cognitive Models

M. B. Guzairov
Department of computer science and robotics
Ufa state aviation technical university
Ufa, Russia
e-mail: guzairov@ugatu.ac.ru

V. I. Vasilyev
Department of computer science and robotics
Ufa state aviation technical university
Ufa, Russia
e-mail: vasilyev@ ugatu.ac.ru

R. T. Kudryavtseva
Department of computer science and robotics
Ufa state aviation technical university
Ufa, Russia
e-mail: cudrt@mail.ru

Abstract[1]

This paper describes the technique of risk evaluation when evaluating the information security (IS) level of an organization. The method is based on the building fuzzy cognitive map (FCM) of organization.

1. Introduction

The information security of organization is a condition of this organization safety from the threats in information sphere. The security is achieved by maintenance of confidentiality, integrity and availability of information resources and existing infrastructure in which information is being processed,

At present, there are a lot of international and national standards and recommendations to provide the certain (required) level of information security (ISO/IEC 15408, ISO/IEC 17799, ISO/IEC 13335, ISO/IEC 27001, ISO/IEC 27002 etc.).

During last ten years the theory and practice of information security rapidly developed in our country. So, the basic document defining the objectives, tasks and mechanisms of information security management at the level of organization should be the Security Policy of the enterprise. The analysis of various approaches to development of security policy shows that the problem is reduced to analysis and management of information risks [1]. The development of corresponding instrumental tools would allow us to choose economically justified approach to IS system design and exploitation.

Proceedings of the 12th international workshop on computer science and information technologies CSIT'2010, Moscow – Saint-Petersburg, Russia, 2010

2. Approaches to estimation and management of information risks

The risk value (R) is defined as the average potential damage from realization of possible threats and is the function of three quotient sets:

$$R = f(U, M, r), \quad (1)$$

where U is the set of possible threats;

M – the set of information system vulnerabilities through which the threats can be realized;

r – the set of protected resources (assets).

In order to estimate the level of enterprise information security it is necessary to analyse and define these three sets. In general case, the formula used to evaluate the risk value R is as follows:

$$R_{\Sigma} = \sum_{i,j} R_{ij} = \sum_{i,j} P_i^U \cdot P_{ij}^V \cdot r_j \ , \quad (2)$$

where R_{ij} is the risk of j-th resource from i-th threat action;

$P^U{}_i$ – the probability of i-th threat appearance;

$P^V{}_{ij}$ – the probability of j-th resource vulnerability relative to i-th threat;

r_j – the value of j-th resource.

The problem essence is to define the probabilities estimates for the threats and vulnerabilities in investigated information system.

In Fig. 1 the basic stages of organization's information risks evaluation are presented.

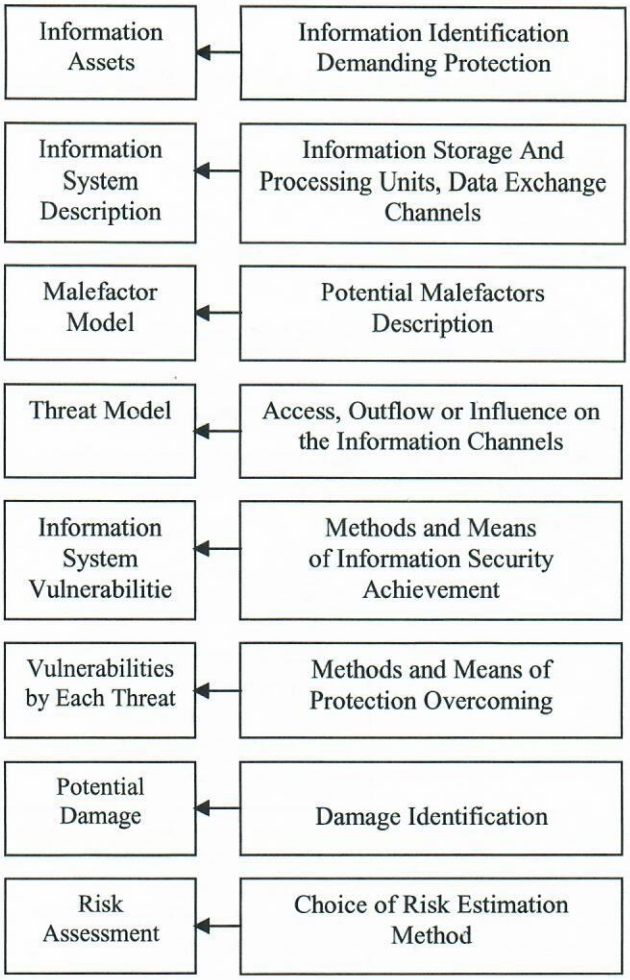

Fig. 1. Basic stages of organization's information risks evaluation

The complexity of information risks assessment consists in the following:

1. The enterprise` information system is a complex distributed system as a rule.
2. There exists usually the high level of information uncertainty.
3. There are a lot of threats and vulnerabilities not taken into account.
4. There exists the high dynamism and large uncertainty of information risk components (threats, vulnerabilities, malefactors).
5. It is difficult to assess a complexity of potential damage from security threats realization.

Therefore, as a rule, the risk assessment problem has a qualitative character that complicates the effective protection system design.

It is important to take into account some features of modern information system influencing the maintenance of information security required level:

- large territorial spread of separate objects included in information system;
- presence of information having different level of confidentiality (open/confidential/commercial information, personal data, etc.);
- non-uniform contingent of users with various level of training having access to information resources;
- use of modern information-communication technologies of various kind;
- mixed document turnover (paper/electronic);
- high level of the "human" factor influence, etc.

Frequently it is difficult to define the damage volume from the loss of used information resources. At the same time, expenditures for information security should be adequate to possible potential losses from the threats realization in information system.

The analysis of risks and expenditures for protection system allows us to define the rational ways of information security management and to justify the required expenditures for security. It is necessary to make decisions on a choice of necessary protection measures and allowable risk level assessment by criterion *"cost – efficiency"*. Thus, the following statements of the problem of protection measures choice are possible:

1. $S_\Sigma \rightarrow \min$ under $R_\Sigma \leq R_{all.}$ – to provide the minimal level of expenditures on the information protection system under condition of allowable risk level maintenance;
2. $R_\Sigma \rightarrow \min$ under $S_\Sigma \leq S_{all.}$ – to minimize the risk under the given level of expenditures on creation of information protection system.

Here: R_Σ and S_Σ are the total risk and expenditures on the information protection measures; $R_{all.}$ and $S_{all.}$ – the allowable limited values of total risk and mentioned expenditures.

In order to estimate the risks decrease level by using the information protection measures, on can use the formula:

$$E = \frac{R'_\Sigma - R_\Sigma}{R'_\Sigma}, \qquad (3)$$

where R'_Σ is the initial risk value;

R_Σ – the risk value after using the additional protection measures.

3. Cognitive approach to complex systems modeling

Last years cognitive modeling methods are more widely applied to solving the problems of analysis and management of complex systems [2]. Cognitive

modelling allows us to investigate the complex system behaviour which is characterized by incomplete or uncertain knowledge of their nature [3].

The concept of "situation" is the basic concept of the given approach. The situation is characterized by the set of basic factors which describe the state of investigated object. Factors can influence on each other, and such influence can be both "positive" when the increase (reduction) of one factor results in increase (reduction) of the other factor, and "negative" when the increase (reduction) of one factor results in reduction (increase) of the other factor.

Thus cognitive maps can be used for factor influence estimation. The cognitive situation map is the weighted directed graph, the units of which are the specified basic factors, and the arcs are the links between them. The cognitive map, in which the influences between the concepts are set by fuzzy variables (for example, «strong influence», «medium influence», «weak influence»), is called as fuzzy cognitive map (FCM).

Generally, a fuzzy cognitive map is a triad of sets:

$$FCM = \{C, F, W\}, \quad (4)$$

where C is the set of concepts (factors);

F – the set of the links between the concepts;

W – the set of the links weights.

Each concept's state is described by one or several state variables. Changing the state of the basic factors with the help of the certain control actions (factors), it is possible to achieve the required state of investigated object (system).

4. Analysis and management of information risks on the basis of cognitive approach

The offered technique of risks evaluation is based on the usage of fuzzy cognitive maps. This allows us to build the adequate model of the object with account of the threats acting the protected resources and the consequences of this action even if the information available is insufficient and contradictory.

To build the corresponding fuzzy cognitive map, it is necessary to fulfil the following stages:

1. Identification of information assets.
2. Evaluation of the identified assets value.
3. Identification of threats and vulnerabilities for involved assets.
4. Estimation of damage in case of possible threats realization.

The process of forming and using FCM for information risks estimation includes the following procedures (Fig. 2):

- definition of the concepts set applied to the object investigated;
- definition of «cause-effect» links (relations) between each pair of concepts;
- building of fuzzy cognitive map;
- dynamic simulation;
- analysis of FCM characteristics (estimation of information risks);
- selection of control actions (measures);
- analysis of control actions efficiency with the purpose of system behaviour optimization.

The tasks of FCM construction and information risks estimation are solved with use of expert estimates method.

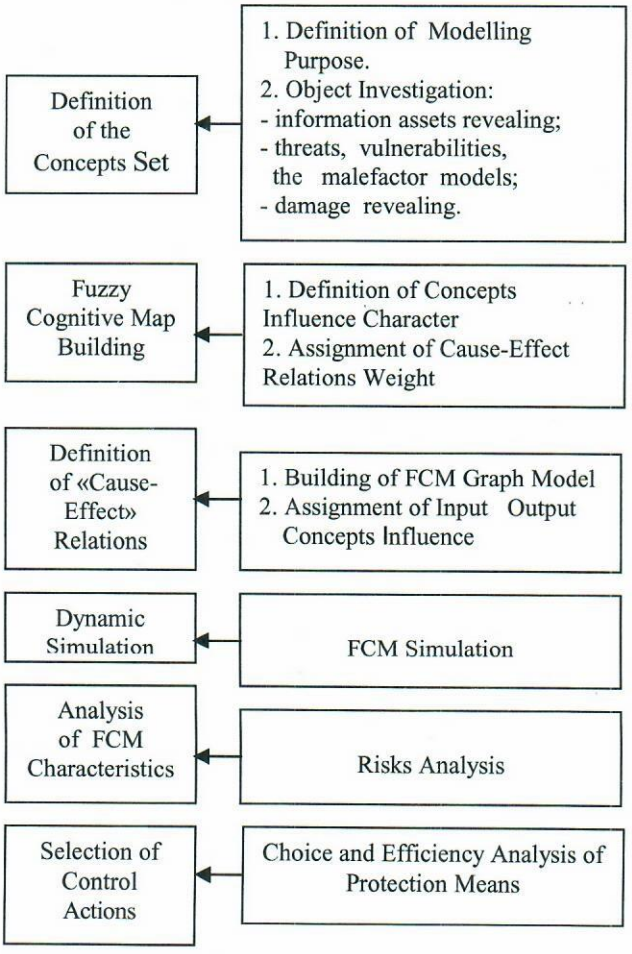

Fig. 2. Stages of FCM building for estimation of information risks

In order to build the fuzzy cognitive map, the following concepts are to be defined:

1. The set of information resources $\{C^S_m\}$ – databases, confidential documents etc.);

2. The set of destabilizing factors (threats) $\{C^U_i\}$ - the loss of privacy, falsification, disclosure, theft of the data;
3. The set of intermediary indicators $\{C^I_l\}$ which show the state of the object security from the point of view of information security level maintenance, confidentiality, integrity and availability of information, emotional and psychological state of the personnel;
4. The set of the objective factors $\{C^G_j\}$ which take into account the quality, status and financial state of investigated enterprise;
5. The set of controlling factors $\{C^R_k\}$ – the means of information protection.

Finally, the fuzzy cognitive map can be presented as the set of the following kind:

$$\text{FCM} = \{C^G_j, C^U_i, C^R_m, C^S_k, C^I_l, W\}, \quad (5)$$

where W is the set of the links weights between the FCM concepts.

The weights of the links in FCM take linguistic terms or interval values. Then the membership functions of corresponding fuzzy sets are interpreted for further simulations.

Using FCM, the total effect $S(\{C^U_i\}\rightarrow C^G_j)$ of threats $\{C^U_i\}$ action to the objective factor C^G_j can be calculated. For this purpose it is necessary to calculate indirect effect $T(C^U_i\rightarrow C^G_j)$ of the threat C^U_i on the objective factor C^G_j, equal to:

$$T(C^U_i\rightarrow C^G_j) = \min\{w_{ij}\}, \quad (6)$$

where $\{w_{ij}\}$ are the weights of the links on the ways between concepts C^U_i and C^G_j.

The total effect is equal to:

$$T(\{C^U_i\}\rightarrow C^G_j) = \max\{T_1, T_2 \ldots, T_N\}, \quad (7)$$

where T_k is the indirect effect between the threat C^U_i and the objective factor C^G_j;

N is the number of indirect effects.

Let's consider the example of estimation of concept C^U_1 (threat) influence on concept C^G_1 (damage) for FCM presented in Fig. 3. For this purpose we shall consider all indirect effects between these concepts $T_n(C^U_1\rightarrow C^G_1)$:

$$\begin{aligned} &T_1(C^U_1\rightarrow C^S_1\rightarrow C^G_1),\\ &T_2(C^U_1\rightarrow C^S_1\rightarrow C^I_1\rightarrow C^G_1),\\ &T_3(C^U_1\rightarrow C^S_2\rightarrow C^G_1),\\ &T_4(C^U_1\rightarrow C^S_2\rightarrow C^I_1\rightarrow C^G_1). \end{aligned} \quad (8)$$

Then we shall obtain:

T_1 = min {strong, medium} = medium;

T_2 = min {strong, medium, medium} = medium;

T_3 = min {medium, strong} = medium;

T_4 = min {medium, strong, medium} = medium.

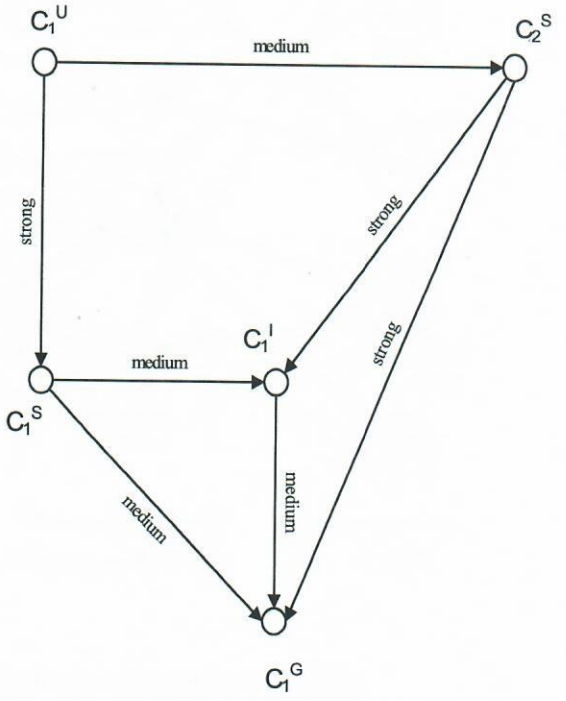

Fig. 3. Determination of threat influence C^U_1 on objective factor C^G_1

The total influence effect of factor C^U_1 on the objective factor C^G_1 will be equall to:

$$T(C^U_1\rightarrow C^G_1) = \max\{T_1, T_2, T_3, T_4\} = \text{medium}. \quad (9)$$

The total effect [1] gives the approximate value of the probability of threat realization and existing vulnerability relative to the given objective factor. The formula given below can be used to calculate the risk value:

$$R_{ij} = T(\{C^U_i\}\rightarrow C^G_j)\cdot r_j, \quad (10)$$

where $T(\{C^U_i\}\rightarrow C^G_j)$ is the total effect of i-th threat action to j-th objective factor calculated with use of FCM;

r_j – the j-th resource value.

The total risk of organization can be calculated using the following formula:

$$R = \sum_{i,j} v_j \cdot R_{ij}, \quad (11)$$

where R_{ij} is the risk of j-th objective factor relative to i-th threat;

v_j – the significance of j-th objective factor calculated by experts.

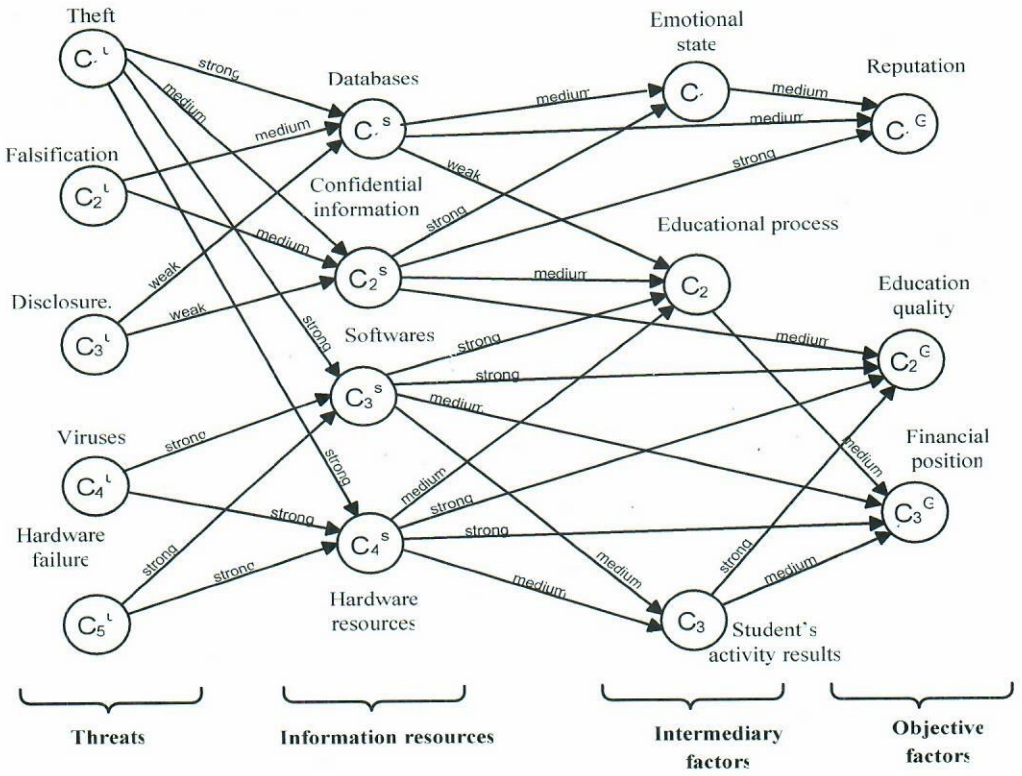

Fig. 4. Fuzzy cognitive map for University's information risks estimation

Table 1. Concepts and their state variables

Concept	Concept name	State variable x_i
C_1^U	Theft	Average thefts quantity
C_2^U	Falsification	Average falsifications quantity
C_3^U	Disclosure	Average disclosures quantity
C_4^U	Viruses	Average viruses quantity
C_5^U	Hardware failure	Average hardware failures quantity
C_1^S	Database	Database information credibility level, %
C_2^S	Confidential information	Confidential information security level, %
C_3^S	Software	Software readiness for service, %
C_4^S	Hardware resources	Hardware resources readiness for service, %
C_1^I	Emotional employee state	Average stress load level
C_2^I	Educational process state	Average educational process breaks quantity
C_3^I	Students activity results	Average students' knowledge level
C_1^G	University's reputation	Average positive/negative publications quantity
C_2^G	Education quality	Qualified graduates quantity, %
C^{3G}	Financial position	Capitalization cost

5. FCM using for analysis and management of organization information risks

In Fig. 4 the example of FCM for security evaluation of the University's information system is presented. The state variables (Table 1) were defined for each concept. As objective factors describing the position of University at the market of educational services, the following factors were selected:

C^G_1 – reputation (image) of University;

C^G_2 – education quality;

C^G_3 – financial position of University.

The basic information resources here are various databases (C^S_1), confidential (C^S_2), software (C^S_3) and hardware resources (C^S_4).

The basic threats are theft (C^U_1), falsification (C^U_2), disclosure of information (C^U_3), viruses attacks (C^U_4), hardware failures (C^U_5).

Intermediary factors (indicators) are emotional state of employee (C^I_1), state of educational process (C^I_2), level of students activity results (C^I_3).

The links weights are defined by three values of linguistic variable such as 'weak', 'medium' and 'strong'(see Table 2).

Table 2. The influence of threats on target factors

Threats (Ci^U)	Total effect of threats influence on objective factors $T(C^U_i \rightarrow C^G_j)$		
	C^G_1	C^G_2	C^G_3
C^U_1	medium	strong	strong
C^U_2	medium	medium	medium
C^U_3	weak	weak	weak
C^U_4	-	strong	strong
C^U_5	-	strong	strong

The software package FCMBuilder for automatization of all stages of FCM building and information risks estimation is developed. In Fig. 5 the results of University's information **risks** estimation are shown.

The created program 'FCMBuilder' allows us to build FCM quickly and evidently, to make calculations by estimation and reassessment of risks, to reveal the largest risks in investigated information system, to estimate the efficiency of information protection measures.

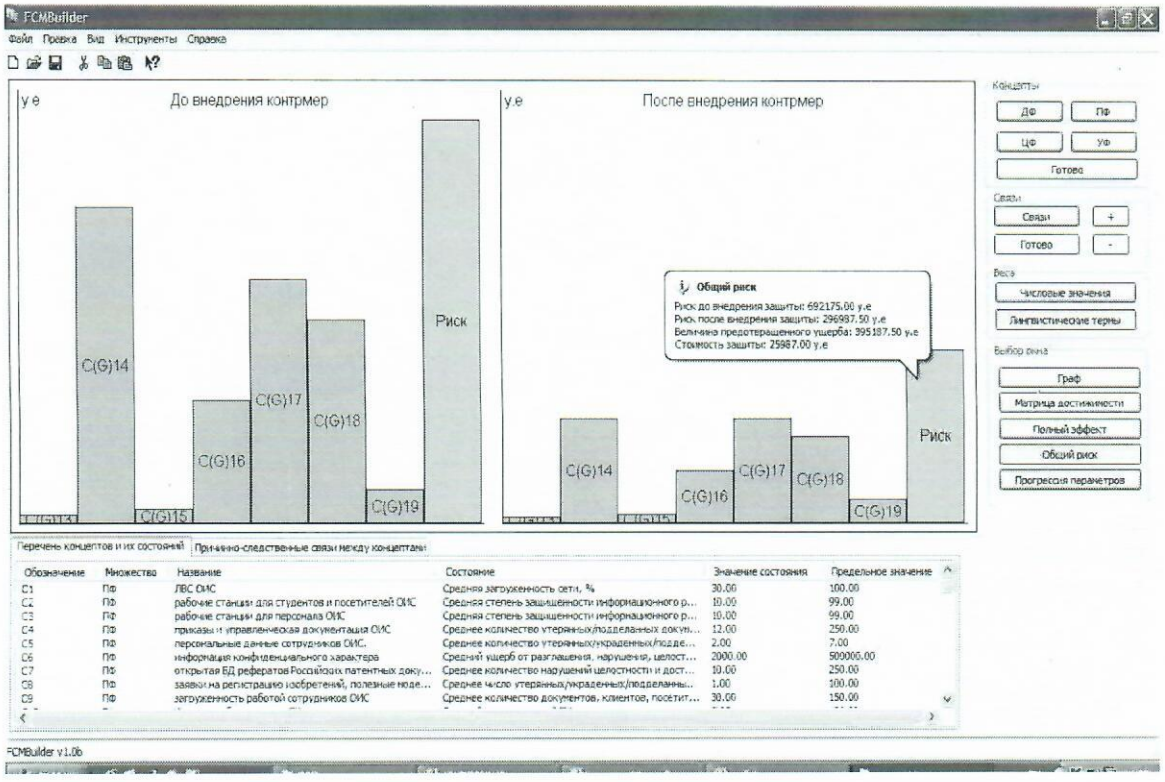

Fig. 5. Results of University's information risks analysis

6. Conclusions

The offered approach to estimation and management of information risks on the basis of fuzzy cognitive maps allows us:

- to estimate the current information security state of enterprise and sufficiency of organizational and technical measures of information protection for maintenance of allowable risks level;
- to reveal the most dangerous threats and vulnerabilities influencing on information system (business processes) of e enterprise;
- to estimate possible damage from threats action on information system of enterprise;
- to state the necessary expenditures estimation for maintenance of required security measures at enterprise;
- to provide the effective mechanisms of decision making of e information security management.

Acknowledgements

This investigation is supported by President of Russian Federation grant HIII 65497.2010.9 for leading scientific schools.

References

1. Petrenko S. A., Simonov S. V. "Information risk management". DMK Press, 2005 (in Russian).
2. Maksimov V. I., Kornoushenko E. K. "Analytical bases of FCM application under solving unstructured problems". IPU Trans., 1998 (in Russian).
3. Kosko B. "Fuzzy Cognitive Maps", International Journal of Man-Machine Studies. Vol. 1. 1986, pp. 65–75.