Assessment and Information Security Provision of the Decision Support Process in Technogenic Object Management Systems

Viktor Perederyi[1], Eugene Borchik[2], Waldemar Wójcik[3] and Oksana Ohnieva[1]

[1]Kherson National Technical University, Beryslavske shose 24, Kherson, 73008, Ukraine
[2]Mykolaiv National Agrarian University, Heorhiia Honhadze street 9, Mykolaiv, 54000, Ukraine
[3]Lublin University of Technology, Nadbystrzycka 38d, Lublin, 20-618, Poland

Abstract

The paper considers the information technology of assessment and provision of complex information security of decision-making process in human-machine management systems for technogenic objects, which complements the theory and methods of solving reliability and survivability problems of multilevel systems, based on the interaction of the set of their workability indicators, human factor and information security indicators in the decision-making process to ensure the efficiency of critical object management.

To assess the impact of a set of indicators of non-factors of information security, external, production, and human factors on the decision-making process of decision-maker in the management of critical objects, a fuzzy Bayesian network was built, which allowed, based on expert knowledge, to assess the probability of the critical object's information security states.

To practically substantiate the obtained results, an experiment was carried out, the results of which confirmed the practical value of the information technology, which can be used to assess and ensure comprehensive information security of the decision support process in man-machine management systems for technogenic objects.

Keywords

Complex multilevel systems, complex organizational and technical objects, decision-maker, functional stability, human factor, relevant decisions, fuzzy risk in decision-making, Bayesian network.

1. Introduction

Currently, when creating and operating complex multilevel systems (CMS) for the management of complex technogenic objects (CTO), the main task is to improve efficiency, which is associated with increasing technical and software complexity. In this regard, the requirements for both the

CITRisk'2021: 2nd International Workshop on Computational & Information Technologies for Risk-Informed Systems, September 16–17, 2021, Kherson, Ukraine
EMAIL: viperkms1@gmail.com (V.Perederyi); borchikeu@gmail.com (E.Borchik); waldemar.wojcik@pollub.pl (WWójcikc); oksana_ognieva@meta.ua (O.Ohnieva)
ORCID: 0000-0002-9241-3034 (V.Perederyi); 0000-0003-0188-1471 (E.Borchik); 0000-0002-6473-9627 (W.Wójcikc); 0000-0001-6206-0285 (O.Ohnieva)


reliability of the components that make up the system and the reliability and performance of the decision-maker (DM) are being raised.

Although the decision-making process is significantly influenced by the human factor, the efficiency and quality of management also depend on the speed and timeliness of receiving the necessary and reliable information about objects and processes by operational and control personnel (OCP) responsible for decision-making in emergencies.

The safe operation of man-machine systems (MMS) depends significantly on information and communication technologies and their cyberinfrastructure. At present, traditional security measures are mainly used, such as authentication, access control, authorization, data encryption, public key infrastructure, firewalls, intrusion detection systems, network security protocols, etc. However, recent cyber attacks on critical systems around the world have shown a significant gap between the ability to protect and restore traditional systems and new security requirements, especially in the context of the intellectualization of the technologies of MMS for the management of critical objects.

Moreover, insufficient attention has been paid to the issues of assessing and providing comprehensive information security for the process of relevant decision making support (RDM), in distributed MMS for management of technogenic objects, associated with the occurrence of hazardous situations under uncertainty and the impact of non-factors on the process of managerial decision-making and implementing due to the imperfection of the mathematical, statistical and intellectual tools used to solve this problem.

Thus, an urgent scientific problem is to improve the functional security of MMS for the management of technogenic objects through the development and implementation of methods and technologies for monitoring, assessment, and provision of comprehensive information security of the RDM support process.

2. Literature review

The solution to this problem is presented in the results of the following scientific studies.

Cybersecurity Risk Assessment [1] states that cybersecurity in the management of a technogenic object is an important issue that can lead to serious hazards in the event of an accident. To assess the cybersecurity risks of nuclear plant control systems, the paper proposes a probabilistic method using the Bayesian network (BN) model and event tree.

In [2] the methods of risk assessment for SCADA systems are considered and analyzed in detail. The essence of methods is described, stages of risk management are considered, the scheme of classification of methods for the estimation of risks of cybersecurity is proposed. In [3], a wide range of threats that lead to cybersecurity risk was studied, a database of actual losses in the event of these threats was created, and a loss analysis was performed using statistical and actuarial mathematics methods. Improving the model of cybersecurity risk assessment using a fuzzy logic apparatus that takes into account four risk factors: vulnerability, threat, probability, and impact was proposed in [4].

In [5-7] methods are proposed that enable determining the total risk of cybersecurity of critical infrastructure, the total damage due to multiple cyber threats, the total amount of damage due to cyber threats over a period of time, the probability of maximum losses as a result actions of cyber threats. It is also noted that the process of identifying and assessing the risk of irrelevant decisions under the influence of cyber threats is the basis and grounds for research in the field of analysis

and improvement of existing and invention of new methods of risk assessment, its accuracy, and applying mathematical operations to risks.

In [8], the human factor was noted to play an important role in modern complex dynamical systems (CDS), in accidents and catastrophes. It is noted that little attention is paid to the problems of risks associated with the informational and cognitive aspects of human-machine interaction. It is recommended that the design and operation of CDS take into account the risks of irrelevant decision-making arising in unpredictable conditions, as well as special requirements for the human psychophysiological state and his or her admission to perform particularly responsible work. It is also noted that the informational and cognitive aspects of human factor engineering play a key role in the safety, reliability, and efficiency of CDS in the management of critical objects.

Therewith, the analysis of the research subject area showed the lack of effective information technology capable of providing comprehensive information security in the process of supporting RDM in the distributed MMS for the management of technogenic objects.

In this regard, to develop the theory of assessment and provision of the effective management of critical objects, we propose the information technology to assess and ensure comprehensive information security of the process of supporting RDM in the MMS for the management of technogenic objects.

3. Problem statement

A review, systematization, and generalization of publications on the analysis, assessment, and management of critical MMS show that in addition to system parameters, the impact of non-factors of the external and production environment on the human factor, management efficiency depends on the impact of information indicators security for the RDM support process during the operation of the system.

Based on the results of the analysis of the literature sources, it is noted that in the RDM support process, the following groups of factors, shown in the information model below, have the most significant impact on the set of information security indicators (Figure 1) [9].

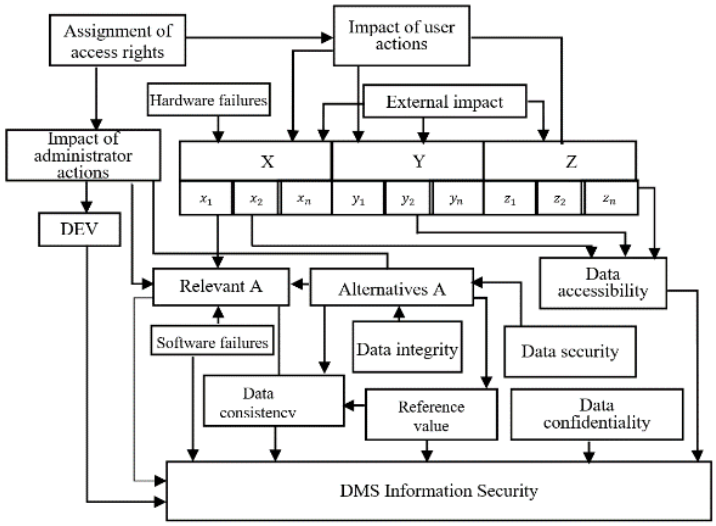

Figure 1: Information model for assessment and provision of comprehensive information security of the decision-making support (DMS) process in the MMS for the management of technogenic objects

Provision of the information security of the RDM support process is characterized by the following important non-factors.

12 - assignment of access rights (privileged) - the process of determining access rights to the DB or DBMS. Privilege is based on a hierarchical structure; it has a flexible scenario that allows maximizing the database security; *N* - the impact of user actions. Unintentional actions lead to changes in parameters and algorithms of system functioning. Intentional actions are aimed at obtaining unauthorized access to information or violation of the system operation; *7.* Hardware failures are equipment failures, physical impacts on the system, and equipment integrity. Having different degrees of protection from external impacts, complete data protection or operability of all system is not guaranteed; *X* - state of the technological process; *Z* - the influence of the external environment on the DM; *Y* - indicators of psychological and mental factors of DM; *E* - software failures; *V* - consistency of data in the database and the relationships between tables; *W* - data availability, correct work with the database; *3* - confidentiality of data in the system and the database, *1* - the integrity of the data stored in the database; *T* - the impact of the actions of administrators, provides an assessment of the negative impact of users with administrator rights on the information in the database and system; *11* - data security, provides an assessment of the security of the database from hacking and data substitution; *5* - reference value - information on the quality of the relational database, which consists in the absence in any respect of foreign keys that refer to non-existent tuples; *D* - risk assessment of making irrelevant decisions; alternatives *(A)* - a sample of relevant alternatives to DMS from KB; *P* - the result of the search for relevant solutions of the RDM, taking into account the relevant impact factors; *R* - state of information security for making relevant decisions by DM.

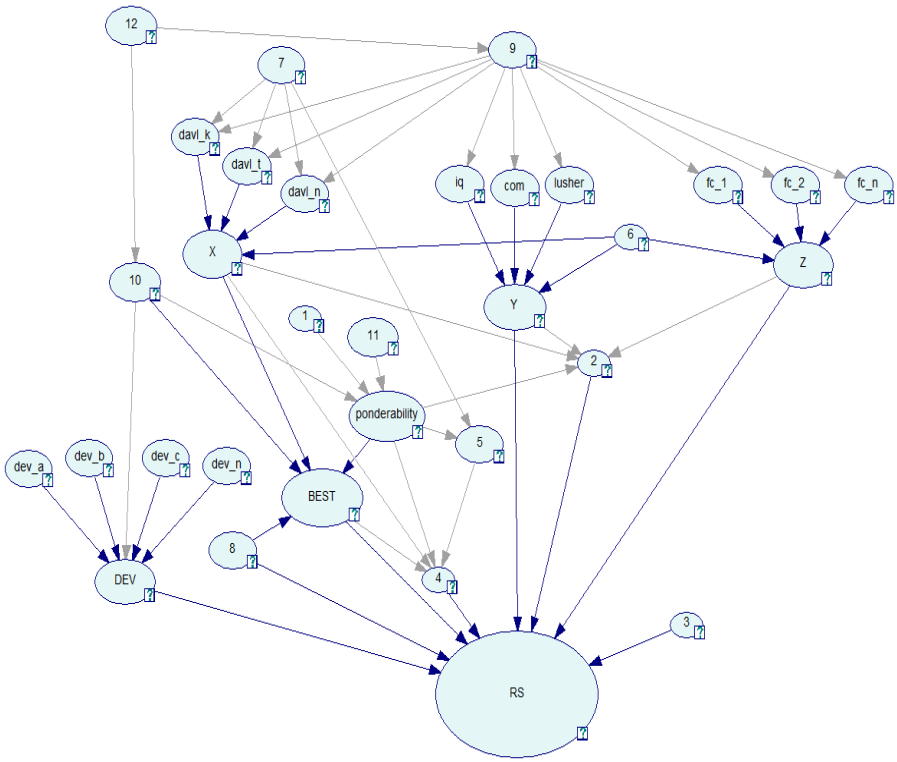

Figure 2: BN for the assessment of comprehensive information security of the DMS process

Since the risk of irrelevant decision making is determined by the simultaneous impact of a set of information security non-factors, one of the stages of its assessment is to identify causal relationships and dependencies between these factors, which will make it possible to assess the change in the probability of risk in the event of a change in the probability of the occurrence of some events. The traditionally used probabilistic approach to uncertainty determination in Bayesian models is not always applicable due to the lack of statistical information about the state of a complex system. To solve this problem, fuzziness was introduced into the BN in the following way [10, 11]. The unconditional and conditional probabilities at the BN's vertices are represented by fuzzy numbers obtained as a result of expert evaluation of a vertex's ability to take a particular value, and the common operations of BN-based calculation are replaced by extended operations on fuzzy numbers [12]. Herewith, the introduction of fuzziness will make it possible to analyze poorly formalized information.

For the assessment of complex information security of the DMS process in the MMS for the management of technogenic objects, the following BN was built (Figure 2).

4. Materials and methods

Figure 3 presents a simplified BN as an example of calculation for a fuzzy Bayesian network. The fuzzy probabilities of variables are obtained based on expert assessment.

The results of the assessment are presented in the form of fuzzy values of conditional probabilities in tables 1-3.

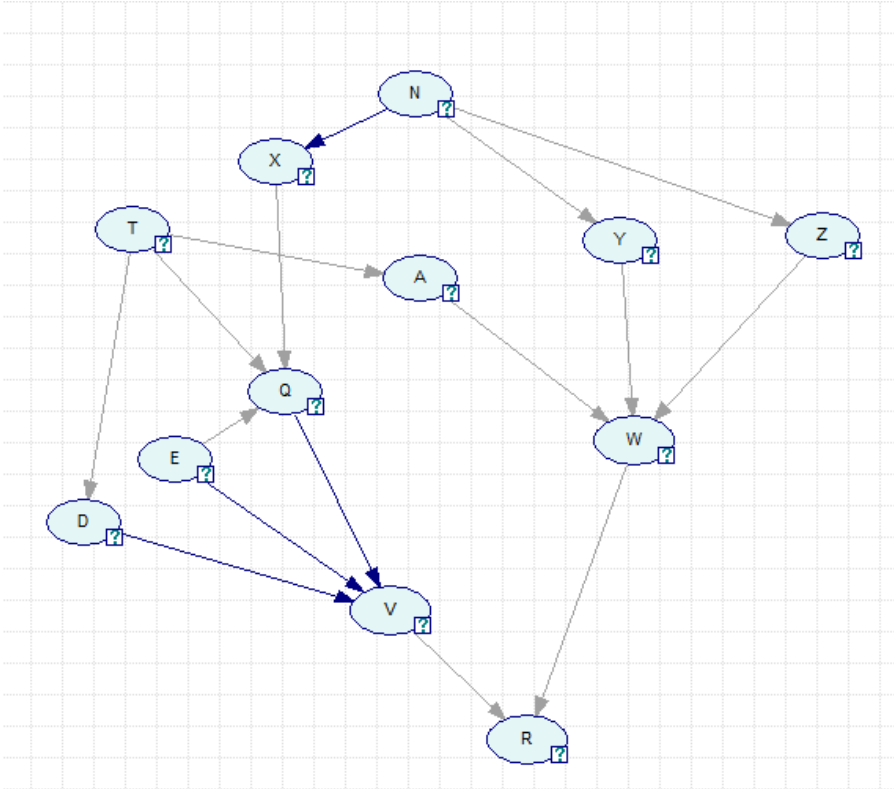

Figure 3: A fragment of a fuzzy BN

It is assumed that all the vertices of the proposed Bayesian network (Figure 3) take only two values.
vertex N takes values n_1 - "low", n_2 - "high";
vertex T takes values t_1 - "low", t_2 - "high";
vertex E takes values e_1 - "does not occur", e_2 - "occur";
vertex X takes values x_1 - "workable", x_2 - "unworkable";
vertex Y takes values y_1 - "norm", y_2 - "non-norm";
vertex Z takes values z_1 - "norm", z_2 - "non-norm";
vertex D takes values d_1 - "low", d_2 - "high";
vertex A takes values a_1 - "sufficient", a_2 - "insufficient";
vertex V takes values v_1 - "consistency", v_2 - "inconsistency";
vertex W takes values w_1 - "sufficient", w_2 - "insufficient";
vertex Q takes values q_1 -"reliable ", q_2 - " unreliable ";
vertex R takes values r_1 -"protected", r_2 - "unprotected"

Since the values of the unconditional probabilities of the root vertices *N, T, E* and the conditional probabilities of the remaining vertices are established on the basis of the results of the expert survey, they are determined vaguely, i.e. are fuzzy sets. Therefore, fuzziness is introduced into the Bayesian network (1) as follows [13].

All unconditional and conditional probabilities of the considered Bayesian network are given in the form of fuzzy trapezoidal numbers $L(l_1, l_2, l_3, l_4)$, having a distribution function set by the formula:

$$\mu_L(x) = \begin{cases} 0, & x < l_1 \quad or \quad x > l_4, \\ \dfrac{x - l_1}{l_2 - l_1}, & l_1 \le x \le l_2, \\ 1, & l_2 \le x \le l_3, \\ \dfrac{l_4 - x}{l_4 - l_3}, & l_3 < x \le l_4, \end{cases}$$

where: $l_1 \le l_2 \le l_3 \le l_4$ – certain real numbers.

A fuzzy trapezoidal number $\widetilde{L}(l_1, l_2, l_3, l_4)$ is also represented [14] as a tuple of four numbers: $\widetilde{L}(a, b, \alpha, \beta)$, where $a=l_2$ and $b=l_3$ - respectively, the lower and upper modal values of the number $\widetilde{L}$; $\alpha = l_2 - l_1$ and $\beta = l_4 - l_3$ – left and right fuzziness coefficients $\widetilde{L}$.

Application of the extension principle to arithmetic operations and trapezoidal fuzzy numbers [14] leads to the following rules for adding and subtracting fuzzy numbers $\widetilde{L}(l_1, l_2, l_3, l_4)$ and $\widetilde{M}(m_1, m_2, m_3, m_4)$ [$\widetilde{L}(a_1, b_1, \alpha_1, \beta_1)$ и $\widetilde{M}(a_2, b_2, \alpha_2, \beta_2)$]:

$$\tilde{L}(l_1, l_2, l_3, l_4) \tilde{\oplus} \tilde{M}(m_1, m_2, m_3, m_4) = \tilde{S}(l_1 + m_1, l_2 + m_2, l_3 + m_3, l_4 + m_4),$$

$$\tilde{L}(a_1, b_1, \alpha_1, \beta_1) \tilde{\otimes} \tilde{M}(a_1, b_1, \alpha_1, \beta_1) = \tilde{H}(a_1 a_2, b_1 b_2, a_1 \alpha_2 + a_2 \alpha_1, b_1 \beta_2 + b_2 \beta_1)$$

It is assumed that the fuzzy numbers are positive, i.e. $l_i \ge 0$, $m_i \ge 0$, $(i = \overline{1, n})$; signs $\tilde{\oplus}$ and $\tilde{\otimes}$ denote the operations of addition and multiplication of fuzzy numbers.

Fuzzy probability under (Ω, ε) is understood [13] as a function $\widetilde{P}_f : \varepsilon \to \widetilde{L}$, that satisfies the following conditions:

1. $\widetilde{0} \prec \widetilde{P}_f(A) \prec \widetilde{1}, \forall A \in \varepsilon$

2. $\widetilde{P}_f(\Omega) = \widetilde{1}$ and $\widetilde{P}_f(\varnothing) = \widetilde{0}$

3. if A and B are inconsistent values from $\varepsilon(A \cap B = \varnothing)$, then $\widetilde{P}_f(A \cup B) = \widetilde{P}_f(A) \widetilde{\oplus} \widetilde{P}_f(B)$

4. if A and B are values from ε, and $\widetilde{\times}$ is a certain fuzzy arithmetic operation, then:

$$\widetilde{P}_f(A) \widetilde{\times} \widetilde{P}_f(B) = \begin{cases} \widetilde{0}, & \text{if } \widetilde{P}_f(A) \widetilde{\times} \widetilde{P}_f(B) \le 0 \\ \widetilde{P}_f(A) \widetilde{\times} \widetilde{P}_f(B), & \text{if } \widetilde{0} \le \widetilde{P}_f(A) \widetilde{\times} \widetilde{P}_f(B) \le \widetilde{1} \\ \widetilde{1}, & \text{if } \widetilde{P}_f(A) \widetilde{\times} \widetilde{P}_f(B) \ge \widetilde{1} \end{cases}$$

Here Ω – is the universal set defining the variable A, ε; is a set of inconsistent numbers A; $\widetilde{L}$ – a set of fuzzy numbers; $\widetilde{0}$ and $\widetilde{1}$ – fuzzy numbers 0 and 1; $(\Omega, \varepsilon, \widetilde{P}_f)$ – fuzzy probability space.

Condition 4) imposes restrictions on the result of fuzzy operations with values of fuzzy probabilities so that condition 1) is guaranteed to be fulfilled.

To compare fuzzy numbers in condition 4), the following approach is used. It is considered, that of two fuzzy numbers, the greater is the one, the defuzzification value of which is greater. For fuzzy numbers $\widetilde{0}$ and $\widetilde{1}$, defuzzification values are taken equal to crisp numbers 0 and 1, respectively.

For the rest of the fuzzy numbers, the center of gravity method is chosen as the defuzzification method, which for trapezoidal fuzzy numbers $\widetilde{L}(l_1, l_2, l_3, l_4)$ takes the following form [14]:

$$L = \frac{\int_{l_1}^{l_4} x\mu(x)dx}{\int_{l_1}^{l_4} \mu(x)dx} = \frac{1}{3} \cdot \frac{-l_1{}^2 - l_2{}^2 + l_3{}^2 + l_4{}^2 - l_1 l_2 + l_3 l_4}{-l_1 - l_2 + l_3 + l_4} \quad (1)$$

where L – defuzzification result, "exact" value of a fuzzy number $\widetilde{L}$.

Table 1

The result of assessing fuzzy conditional probabilities at nodes X, Y, Z, D, A

N	$\tilde{P}_f(X = x_1 \mid N)$	$\tilde{P}_f(X = x_2 \mid N)$	N	$\tilde{P}_f(Y = y_1 \mid N)$	$\tilde{P}_f(Y = y_2 \mid N)$
n_1	(0.7; 0.8; 0.9; 1.0)	(0.0; 0.1; 0.2; 0.3)	n_1	(0.8; 0.85; 0.95 ;1.0)	(0.00; 0.05; 0.15; 0.2)
n_2	(0.1; 03; 0.5; 0.7)	(0.3; 0.5; 0.7; 0.9)	n_2	(0.1; 0.2; 0.4; 0.5)	(0.5 0.6; 0.8; 0.9)
N	$\tilde{P}_f(Z = z_1 \mid N)$	$\tilde{P}_f(Z = z_2 \mid N)$	T	$\tilde{P}_f(D = d_1 \mid T)$	$\tilde{P}_f(D = d_2 \mid T)$
n_1	(0.7; 0.8; 0.9; 1.0)	(0.0; 0.1; 0.2; 0.3)	t_1	(0.75; 0.8; 0.9; 0.95)	(0.05; 0.1; 0.2; 0.25)
n_2	(0.5; 0.6; 0.8; 0.9)	(0.1; 0.2; 0.4; 0.5)	t_2	(0.1; 0.2; 0.4; 0.5)	(0.5; 0.6; 0.8; 0.9)
T	$\tilde{P}_f(A = a_1 \mid T)$	$\tilde{P}_f(A = a_2 \mid T)$			
t_1	(0.6; 0.7; 0.9; 1.0)	(0.00; 0.1; 0.3; 0.4)			
t_2	(0.1; 0.2; 0.4; 0.5)	(0.5; 0.6; 0.8; 0.9)			

When calculating fuzzy probabilities in Bayesian network vertices, the following expressions are used [12]:

$$\tilde{P}_f(A_1,...,A_n) \cong \tilde{\bigotimes}_{i=1}^{n} \tilde{P}_f(A_i, Parents(A_i)),$$

where *Parents(Ai)* are parent variables of the variable A_i. The latter expression is called the chain rule for the fuzzy joint probability distribution;

$$\tilde{P}_f(B=b_j, A=a_i) \cong \tilde{P}_f(A=a_i) \tilde{\otimes} \tilde{P}_f(B=b_j \mid A=a_i) \quad -$$

fuzzy joint probability;

$$\tilde{P}_f(B=b_j) \cong \tilde{\bigoplus}_{i=1}^{n} \tilde{P}_f(A=a_i) \tilde{\otimes} \tilde{P}_f(B=b_j \mid A=a_i) \quad -$$

fuzzy composite probability.

Lower-level experts were proposed to assess the conditional probabilities of possible states of the monitoring and control modules of the system's functional sustainability (FS) in the process of its operation. The results are presented in the form of fuzzy values of conditional probabilities in Tables 1-3.

Table 2

The result of assessing fuzzy conditional probabilities at node *R*

V	W	$\tilde{P}_f(R=r_1 \mid V,W)$	$\tilde{P}_f(R=r_2 \mid V,W)$
v_1	w_1	(0.9; 0.95; 0.95; 1.0)	(0.0; 0.05; 0.05; 0.1)
v_1	w_2	(0.4; 0.5; 0.7; 0.8)	(0.2; 0.3; 0.5; 0.6)
v_2	w_1	(0.5; 0.6; 0.8; 0.9)	(0.1; 0.2; 0.4; 0.5)
v_2	w_2	(0.2; 0.3; 0.5; 0.6)	(0.4; 0.5; 0.7; 0.8)

Table 3

The result of assessing fuzzy conditional probabilities at nodes *Q, V, W*

X	T	E	$\tilde{P}_f(Q=q_1 \mid X,T,E)$	$\tilde{P}_f(Q=q_2 \mid X,T,E)$
x_1	t_1	e_1	(0.9; 0.95; 0.95; 1.0)	(0.0; 0.05; 0.05; 0.1)
x_1	t_1	e_2	(0.6; 0.75; 0.85; 1.0)	(0.00; 0.15; 0.25; 0.4)
x_1	t_2	e_1	(0.6; 0.7; 0.7; 0.9)	(0.1; 0.3; 0.3; 0.4)
x_1	t_2	e_2	(0.4; 0.5; 0.7; 0.8)	(0.2; 0.3; 0.5; 0.6)
x_2	t_1	e_1	(0.6; 0.7; 0.9; 1.0)	(0.0; 0.1; 0.3; 0.4)
x_2	t_1	e_2	(0.5; 0.6; 0.8; 0.9)	(0.1; 0.2;0.4; 0.5)
x_2	t_2	e_1	(0.4; 0.5; 0.7; 0.8)	(0.2; 0.3; 0.5; 0.6)
x_2	t_2	e_2	(0.3; 0.5; 0.6; 0.8)	(0.2; 0.4; 0.5; 0.7)
D	E	Q	$\tilde{P}_f(V=v_1 \mid D,E,Q)$	$\tilde{P}_f(V=v_2 \mid D,E,Q)$
d_1	e_1	q_1	(0.9; 0.95; 0.95; 1.0)	(0.0; 0.05; 0.05; 0.1)

d_1	e_1	q_2	(0.8; 0.85; 0.95; 1.0)	(0.00; 0.05; 0.15; 0.2)
d_1	e_2	q_1	(0.8; 0.85; 0.95; 1.0)	(0.00; 0.05; 0.15; 0.2)
d_1	e_2	q_2	(0.7; 0.8; 0.9; 1.0)	(0.0; 0.1; 0.2; 0.3)
d_2	e_1	q_1	(0.4; 0.55; 0.65; 0.8)	(0.2; 0.35; 0.45; 0.6)
d_2	e_1	q_2	(0.3; 0.4; 0.5; 0.6)	(0.4; 0.5; 0.6; 0.7)
d_2	e_2	q_1	(0.4; 0.5; 0.7; 0.8)	(0.2; 0.3; 0.5; 0.6)
d_2	e_2	q_2	(0.2; 0.3; 0.5; 0.6)	(0.4; 0.5; 0.7; 0.8)
A	Y	Z	$\tilde{P}_f(W = w_1 \mid A, Y, Z)$	$\tilde{P}_f(W = w_2 \mid A, Y, Z)$
a_1	y_1	z_1	(0.9; 0.95; 0.95; 1.0)	(0.0; 0.05; 0.05; 0.1)
a_1	y_1	z_2	(0.8; 0.9; 0.9; 1.0)	(0.0; 0.1; 0.1; 0.2)
a_1	y_2	z_1	(0.8; 0.9; 0.9; 1.0)	(0.0; 0.1; 0.1; 0.2)
a_1	y_2	z_2	(0.7; 0.8; 0.9; 1.0)	(0.0; 0.1; 0.2; 0.3)
a_2	y_1	z_1	(0.5; 0.6; 0.8; 0.9)	(0.1; 0.2;0.4; 0.5)
a_2	y_1	z_2	(0.5; 0.6; 0.7; 0.8)	(0.2; 0.3; 0.4; 0.5)
a_2	y_2	z_1	(0.5; 0.6; 0.7 0.8)	(0.2; 0.3; 0.4; 0.5)
a_2	y_2	z_2	(0.4; 0.5; 0.7; 0.8)	(0.2; 0.3; 0.5; 0.6)

The procedure for calculating the value of probabilities of a fuzzy Bayesian network includes the following stages. At the first stage, fuzzy unconditional probabilities of vertices *X, Y, Z, D, A* that have one parent vertex are calculated as follows:

$$\tilde{P}_f(X = x_i) = \tilde{\bigoplus_N} \tilde{P}_f(N, X = x_i) = \tilde{\bigoplus_{k=1}^{2}} \tilde{P}_f(N = n_k, X = x_i) =$$

$$= \tilde{\bigoplus_{k=1}^{2}} \tilde{P}_f(N = n_k) \tilde{\otimes} \tilde{P}_f(X = x_i \mid N = n_k),$$

$$\tilde{P}_f(Y = y_i) = \tilde{\bigoplus_{k=1}^{2}} \tilde{P}_f(N = n_k) \tilde{\otimes} \tilde{P}_f(Y = y_i \mid N = n_k),$$

$$\tilde{P}_f(Z = z_i) = \tilde{\bigoplus_{k=1}^{2}} \tilde{P}_f(N = n_k) \tilde{\otimes} \tilde{P}_f(Z = z_i \mid N = n_k), \qquad (2) \qquad (2)$$

$$\tilde{P}_f(D = d_i) = \tilde{\bigoplus_{k=1}^{2}} \tilde{P}_f(T = t_k) \tilde{\otimes} \tilde{P}_f(D = d_i \mid T = t_k),$$

$$\tilde{P}_f(A = a_i) = \tilde{\bigoplus_{k=1}^{2}} \tilde{P}_f(T = t_k) \tilde{\otimes} \tilde{P}_f(A = a_i \mid T = t_k), \quad (i = \overline{1,2}).$$

At the second stage, fuzzy unconditional probabilities of vertices *Q, V, W* having three parent vertices are calculated as follows:

$$\tilde{P}_f(Q=q_i)=\tilde{\bigoplus_{X,T,E}}\tilde{P}_f(X,T,E,Q=q_i)=$$
$$=\tilde{P}_f(X=x_1,T=t_1,E=e_1,Q=q_i)\tilde{\oplus}\tilde{P}_f(X=x_1,T=t_1,E=e_2,Q=q_i)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(X=x_1,T=t_2,E=e_1,Q=q_i)\tilde{\oplus}\tilde{P}_f(X=x_1,T=t_2,E=e_2,Q=q_i)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(X=x_2,T=t_1,E=e_1,Q=q_i)\tilde{\oplus}\tilde{P}_f(X=x_2,T=t_1,E=e_2,Q=q_i)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(X=x_2,T=t_2,E=e_1,Q=q_i)\tilde{\oplus}\tilde{P}_f(X=x_2,T=t_2,E=e_2,Q=q_i)=$$
$$=\tilde{P}_f(x_1)\tilde{\otimes}\tilde{P}_f(t_1)\tilde{\otimes}\tilde{P}_f(e_1)\tilde{\otimes}\tilde{P}_f(q_i\mid x_1,t_1,e_1)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(x_1)\tilde{\otimes}\tilde{P}_f(t_1)\tilde{\otimes}\tilde{P}_f(e_2)\tilde{\otimes}\tilde{P}_f(q_i\mid x_1,t_1,e_2)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(x_1)\tilde{\otimes}\tilde{P}_f(t_2)\tilde{\otimes}\tilde{P}_f(e_1)\tilde{\otimes}\tilde{P}_f(q_i\mid x_1,t_2,e_1)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(x_1)\tilde{\otimes}\tilde{P}_f(t_2)\tilde{\otimes}\tilde{P}_f(e_2)\tilde{\otimes}\tilde{P}_f(q_i\mid x_1,t_2,e_2)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(x_2)\tilde{\otimes}\tilde{P}_f(t_1)\tilde{\otimes}\tilde{P}_f(e_1)\tilde{\otimes}\tilde{P}_f(q_i\mid x_2,t_1,e_1)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(x_2)\tilde{\otimes}\tilde{P}_f(t_1)\tilde{\otimes}\tilde{P}_f(e_2)\tilde{\otimes}\tilde{P}_f(q_i\mid x_2,t_1,e_2)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(x_2)\tilde{\otimes}\tilde{P}_f(t_2)\tilde{\otimes}\tilde{P}_f(e_1)\tilde{\otimes}\tilde{P}_f(q_i\mid x_2,t_2,e_1)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(x_2)\tilde{\otimes}\tilde{P}_f(t_2)\tilde{\otimes}\tilde{P}_f(e_2)\tilde{\otimes}\tilde{P}_f(q_i\mid x_2,t_2,e_2)\quad, \tag{3}$$

$$\tilde{P}_f(V=v_i)=\tilde{\bigoplus_{D,E,Q}}\tilde{P}_f(D,E,Q,V=v_i)=$$
$$=\tilde{P}_f(D=d_1,E=e_1,Q=q_1,V=v_i)\tilde{\oplus}\tilde{P}_f(D=d_1,E=e_1,Q=q_2,V=v_i)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(D=d_2,E=e_1,Q=q_1,V=v_i)\tilde{\oplus}\tilde{P}_f(D=d_2,E=e_1,Q=q_2,V=v_i)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(D=d_2,E=e_2,Q=q_1,V=v_i)\tilde{\oplus}\tilde{P}_f(D=d_2,E=e_2,Q=q_2,V=v_i)=$$
$$==\tilde{P}_f(d_1)\tilde{\otimes}\tilde{P}_f(e_1)\tilde{\otimes}\tilde{P}_f(q_1)\tilde{\otimes}\tilde{P}_f(v_i\mid d_1,e_1,q_1)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(d_1)\tilde{\otimes}\tilde{P}_f(e_1)\tilde{\otimes}\tilde{P}_f(q_2)\tilde{\otimes}\tilde{P}_f(v_i\mid d_1,e_1,q_2)\tilde{\oplus}$$

$$\tilde{\oplus}\tilde{P}_f(d_1)\tilde{\otimes}\tilde{P}_f(e_2)\tilde{\otimes}\tilde{P}_f(q_1)\tilde{\otimes}\tilde{P}_f(v_i\mid d_1,e_2,q_1)\tilde{\oplus} \tag{4}$$
$$\tilde{\oplus}\tilde{P}_f(d_1)\tilde{\otimes}\tilde{P}_f(e_2)\tilde{\otimes}\tilde{P}_f(q_2)\tilde{\otimes}\tilde{P}_f(v_i\mid d_1,e_2,q_2)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(d_2)\tilde{\otimes}\tilde{P}_f(e_1)\tilde{\otimes}\tilde{P}_f(q_1)\tilde{\otimes}\tilde{P}_f(v_i\mid d_2,e_1,q_1)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(d_2)\tilde{\otimes}\tilde{P}_f(e_1)\tilde{\otimes}\tilde{P}_f(q_2)\tilde{\otimes}\tilde{P}_f(v_i\mid d_2,e_1,q_2)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(d_2)\tilde{\otimes}\tilde{P}_f(e_2)\tilde{\otimes}\tilde{P}_f(q_1)\tilde{\otimes}\tilde{P}_f(v_i\mid d_2,e_2,q_1)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(d_2)\tilde{\otimes}\tilde{P}_f(e_2)\tilde{\otimes}\tilde{P}_f(q_2)\tilde{\otimes}\tilde{P}_f(v_i\mid d_2,e_2,q_2)\,, \tag{5}$$

At the third stage, fuzzy unconditional probabilities of a leaf vertex *R* which has two parent vertices are calculated as follows:

$$\tilde{P}_f(R=r_i)=\tilde{\bigoplus_{V,W}}\tilde{P}_f(V,W,R=r_i)=$$
$$=\tilde{P}_f(V=v_1,W=w_1,R=r_i)\tilde{\oplus}\tilde{P}_f(V=v_1,W=w_2,R=r_i)\tilde{\oplus}$$

$$\tilde{\oplus}\tilde{P}_f(V=v_2,W=w_1,R=r_i)\tilde{\oplus}\,\tilde{P}_f(V=v_2,W=w_2,R=r_i)=$$
$$==\tilde{P}_f(v_1)\tilde{\otimes}\,\tilde{P}_f(w_1)\tilde{\otimes}\,\tilde{P}_f(r_i\,|\,v_1,w_1)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(v_1)\tilde{\otimes}\,\tilde{P}_f(w_2)\tilde{\otimes}\,\tilde{P}_f(r_i\,|\,v_1,w_2)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(v_2)\tilde{\otimes}\,\tilde{P}_f(w_1)\tilde{\otimes}\,\tilde{P}_f(r_i\,|\,v_2,w_1)\tilde{\oplus}$$
$$\tilde{\oplus}\tilde{P}_f(v_2)\tilde{\otimes}\,\tilde{P}_f(w_2)\tilde{\otimes}\,\tilde{P}_f(r_i\,|\,v_2,w_2),\qquad(i=\overline{1,2}). \tag{6}$$

5. Experiment

For the practical evaluation of the proposed models, the following experiment was carried out.

Let information security be influenced by the actions of users (factor N) and administrators (factor T) in the system and database with a low probability value, and software failure (factor E) is of low probability. The result of estimating the probability of the influence of the above factors is presented in the form of fuzzy probabilities $\widetilde{P}_f(N),\widetilde{P}_f(T),\widetilde{P}_f(E)$, given by trapezoidal fuzzy numbers in Table 4. Taking into account the expert estimates of the conditional probabilities of the mutual influence of the factors presented in Tables 1-3, calculations of fuzzy probability values of the considered network nodes are performed using formulas (2-6) in the MATLAB environment. In addition, formula (1) calculates the defuzzification values of fuzzy probabilities at the nodes of the network. The calculation results are presented in Table 4.

As it is seen from Table 4, the probability that the information security is in the "protected" state $P(R=r_1)=0.97$, which, following the regulatory recommendations ($P(R=r_1)\geq 0.95$), is considered as a sufficient value.

Table 4

Results of probability calculation in the nodes of fuzzy BN in the first case

N			T		
	Fuzzy probability value	Defuzzification result		Fuzzy probability value	Defuzzification result
	$\tilde{P}_f(N)$	$P(N)$		$\tilde{P}_f(T)$	$P(T)$
n_1	(0.8; 0.85; 0.95; 1.0)	0.9	t_1	(0.8; 0.85; 0.95; 1.0)	0.9
n_2	(0.0; 0.05; 0.15; 0.2)	0.1	t_2	(0.0; 0.05; 0.15; 0.2)	0.1
	E			X	
	$\tilde{P}_f(E)$	$P(E)$		$\tilde{P}_f(X)$	$P(X)$
e_1	(0.6; 0.7; 0.9; 1.0)	0.8	x_1	(0.41;0.83;0.93;1.12)	0.81
e_2	(0.0; 0.1; 0.3; 0.4)	0.2	x_2	(0.0; 0.11; 0.3; 0.44)	0.21
	Y			Z	
	$\tilde{P}_f(Y)$	$P(Y)$		$\tilde{P}_f(Z)$	$P(Z)$
y_1	(0.63; 0.73; 0.96; 1.09)	0.85	z_1	(0.55; 0.71; 0.97; 1.17)	0.85

y_2	(0.01; 0.07; 0.26; 0.35)	0.17	z_2	(0.01;0.09; 0.25; 0.38)	0.18
	D			A	
	$\tilde{P}_f(D)$	$P(D)$		$\tilde{P}_f(A)$	$P(A)$
d_1	(0.59; 0.69; 0.91; 1.04)	0.81	a_1	(0.47; 0.61; 0.91; 1.09)	0.77
d_2	(0.03; 0.11; 0.31; 0.42)	0.22	a_2	(0.01; 0.11; 0.41; 0.56)	0.27
	Q			V	
	$\tilde{P}_f(Q)$	$P(Q)$		$\tilde{P}_f(V)$	$P(V)$
q_1	(0.58; 0.82; 0.97; 1.33)	0.93	v_1	(0.43;0.79;0.91;1.54)	0.94
q_2	(0.02; 0.03; 0.13; 0.26)	0.11	v_2	(0.0; 0.04; 0.11; 0.28)	0.12
	W			R	
	$\tilde{P}_f(W)$	$P(W)$		$\tilde{P}_f(R)$	$P(R)$
w_1	(0.56; 0.81; 0.96; 1.42)	0.95	r_1	(0.36; 0.83; 0.95; 1.66)	0.97
w_2	(0.01; 0.04; 0.08; 0.15)	0.07	r_2	(0.02; 0.05; 0.07; 0.13)	0.07

Suppose that information security is influenced by the actions of users (factor *N*) and the administrator (factor *T*) on information in the system and the database with a probability value much greater than in the first case, and the failure of the software (factor *E*) is quite probable. The result of evaluating the probabilities of factors *N, T, E* by experts is presented in the form of fuzzy probabilities $\widetilde{P}_f(N), \widetilde{P}_f(T), \widetilde{P}_f(E)$ given by trapezoidal fuzzy numbers in Table 5.

The results of calculating the values of the fuzzy probability of the nodes of the network under consideration are presented in Table 5. As it is seen from Table 5 the probability that the information security is in the "protected" state $P(R=r_1)=0.77$. Consequently, in this case, it cannot be assumed that the information security is in the "protected" state.

Table 5

Results of probability calculation in the nodes of fuzzy BN in the second case

	N			T	
	Fuzzy probability value	Defuzzification result		Fuzzy probability value	Defuzzification result
	$\tilde{P}_f(N)$	$P(N)$		$\tilde{P}_f(T)$	$P(T)$
n_1	(0.5; 0.55; 0.65; 0.7)	0.6	t_1	(0.2; 0.5; 0.6; 0.8)	0.55
n_2	(0.3; 0.35; 0.45; 0.5)	0.4	t_2	(0.2; 0.4; 0. 5; 0.7)	0.45
	E			X	
	$\tilde{P}_f(E)$	$P(E)$		$\tilde{P}_f(X)$	$P(X)$
e_1	(0.5; 0.6; 0.8; 0.9)	0.7	x_1	(0.37;0.55;0.81;1.04)	0.69
e_2	(0.1; 0.2; 0.4; 0.5)	0.3	x_2	(0.07; 0.23; 0.45; 0.65)	0.35
	Y			Z	

	$\tilde{P}_f(Y)$	$P(Y)$		$\tilde{P}_f(Z)$	$P(Z)$
y_1	(0.42; 0.54; 0.8; 0.94)	0.68	z_1	(0.49; 0.65; 0.95; 1.14)	0.81
y_2	(0.14; 0.24; 0.46; 0.58)	0.35	z_2	(0.02; 0.13; 0.31; 0.45)	0.22
	D			A	
	$\tilde{P}_f(D)$	$P(D)$		$\tilde{P}_f(A)$	$P(A)$
d_1	(0.25; 0.68; 0.84; 1.08)	0.7	a_1	(0.09; 0.43; 0.74; 1.11)	0.59
d_2	(0.08; 0.19; 0.41; 0.54)	0.31	a_2	(0.12; 0.36; 0.48; 0.63)	0.4
	Q			V	
	$\tilde{P}_f(Q)$	$P(Q)$		$\tilde{P}_f(V)$	$P(V)$
q_1	(0.37; 0.64; 0.75; 1.32)	0.79	v_1	(0.33; 0.68; 0.92; 1.34)	0.82
q_2	(0.07; 0.17; 0.28; 0.41)	0.23	v_2	(0.04; 0.15; 0.6; 0.39)	0.21
	W			R	
	$\tilde{P}_f(W)$	$P(W)$		$\tilde{P}_f(R)$	$P(R)$
w_1	(0.27; 0.66; 0.87; 1.4)	0.81	r_1	(0.27; 0.69; 0.8; 1.29)	0.77
w_2	(0.03; 0.11; 0.31; 0.42)	0.22	r_2	(0.04; 0.15; 0.38; 0.49)	0.27

6. Conclusions

The information technology was proposed for the assessment and provision of complex information security of decision-making support process in man-machine systems for the management of technogenic objects, which complements the theory and methods of solving the issues of maintaining reliability and survivability of multilevel systems, based on the interaction of its workability indicator set, human factor and the indicators of information security in the decision-making process, to ensure the management efficiency of critical objects.

To assess the impact of a set of indicators of information security non-factors, as well as external, production, and human factors on the decision-making process of DM in the management of critical objects, a fuzzy BN was proposed. A fuzzy BN was proposed to assess the complex information security of the DMS process in the MMS for managing a technogenic object. An algorithm for calculating fuzzy probabilities of the nodes of this network was developed. In the MATLAB environment, a numerical experiment was carried out for various values of the degrees of influence of factors on the information system.

Thus, if the impact on the information security of users (factor N) and the administrator (factor T), as well as software failure (factor E), are unlikely, then information security with a sufficient degree of probability is in a protected state. If the impact on the information security of users (factor N) and the administrator (factor T), as well as software failure (factor E), are quite probable, then information security is in a protected state with an insufficient degree of probability, that is, it is not protected. To bring it into a protected state, it is necessary to reduce the degree of impact of negative factors T, N, E on it to a certain level. Thus, the fuzzy model built for analyzing the impact of non-factors on the degree of information security allows assessing the degree of its protection, taking into account the causal relationships of these factors.

References

[1] J.Shin., H.Son, G.Heo, Cyber security risk evaluation of a nuclear I&C using BN and ET, Nuclear Engineering and Technology, No. 49(3), 2017, pp.517–524. https://doi.org/10.1016/j.net.2016.11.004

[2] Yu.Cherdantseva, P.Burnap, A.Blyth, P.Eden, K.Jones, H.Soulsby, K.Stoddart, A review of cyber security risk assessment methods for SCADA systems, Computers & Security, No. 56, 2016, pp.1–27. https://doi.org/10.1016/j.cose.2015.09.009

[3] M.Eling, J.Wirfs, What are the actual costs of cyber risk events? European Journal of Operational Research, No. 272(3), 2019, pp.1109–1119. DOI: 10.1016/j.ejor.2018.07.021

[4] M.Alali, A.Almogren, H.M.Mehedi, I.Rassan, A.Z.Bhuiyan, Improving risk assessment model of cyber security using fuzzy logic inference system, Computers & Security, No. 74, 2018, pp.323–339. DOI:10.1016/j.cose.2017.09.011

[5] A.Terje, Risk assessment and risk management: Review of recent advances on their foundation, European Journal of Operational Research, Volume 253, No. 1, 2016, pp. 1–13. https://doi.org/10.1016/j.ejor.2015.12.023

[6] P.Jain, H.J.Pasman, S.Waldram, E.N.Pistikopoulos, M.S.Mannan, Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management, Journal of Loss Prevention in the Process Industries, Volume 53, 2018, pp. 61–73. https://doi.org/10.1016/j.jlp.2017.08.006

[7] V.Mokhor, O.Bakalynskyi, O.Bohdanov, V.Tsurkan, Interpretation of the simple risk level dependence of its implementation in the terms of analytic geometry, Information technology, and security. Volume 5, No. 1, 2017, pp. 71–82. DOI:10.20535/2411-1031.2017.5.1.120574

[8] G.Mygal, V.Mygal, Interdisciplinary approach to the human factor problem, Municipal economy of cities? No. 3, 2020, pp.149-157. 10.33042/2522-1809-2020-3-156-149-157

[9] V.Perederyi, E.Borchik, O.Ohnieva, Information Technology of Control and Support for Functional Sustainability of Distributed Man-Machine Systems of Critical Application, Lecture Notes in Computational Intelligence and Decision Making.Proceedings of the XV International Scientific Conference “Intellectual Systems of Decision Making and Problems of Computational Intelligence” (ISDMCI'2019), Ukraine, May 21–25, 2019, pp. 461-477. https://doi.org/10.1007/978-3-030-26474-1_33

[10] J.Ren, J.Wang, I.Jenkinson, D.L.Xu, J.B.Yang, An offshore risk analysis method based on fuzzy Bayesian networks, EPSRC report, 2005.

[11] C.Fogelberg, Fuzzy bayesian networks for network inference, Transfer Report, Computing Laboratory, Wolfson Building, Parks Road, Oxford, OX13QD, October 2008

[12] H.Pan, L.Liu, Fuzzy Bayesian networks – a general formalism for representation, inference and learning with hybrid Bayesian networks, IJPRAI, Vol.14(7), 2000, pp. 941–962

[13] J.Halliwell, J.Keppens, Q.Shen, Linguistic Bayesian networks for reasoning with subjective probabilities in forensic statistics, Proc. of the 5th International Confer-ence on AI and Law, 2003, pp. 42–50

[14] A.V.Leonenkov, Fuzzy modeling in MATLAB and fuzzyTECH, St. Petersburg: BHV-Petersburg, 2005, 736 p