KYBERNETIKA — VOLUME *51* (2015), NUMBER 3, PAGES 408–419

IT/IS SECURITY MANAGEMENT WITH UNCERTAIN INFORMATION

Cyril Klimeš and Jiří Bartoš

The paper introduces a novel proposal of a security management system destined primarily for application in the field of IT. Its core is formed by a triplet of cooperating knowledge-based (expert) systems, the knowledge bases of which consist of vague If-Then rules. The knowledge bases were created by experts on the problem domain and multiple times tested and verified on actual scenarios and real systems. With the system, a comprehensive methodology that is a part of a more complex approach to a decision making process is introduced. The proposed fuzzy tool is demonstrated on examples and problems from the area of information security. The paper also briefly reviews other used approaches to information security management – mainly qualitative and quantitative methodologies.

Keywords: information retrieval, fuzzy sets, modeling information systems under uncertainty, adaptive model, information security, risk management, risk analysis

Classification: 93E12, 62A10

1. INTRODUCTION

Risk analysis is an essential part of IT/IS security management. For this, two basic types of methods are usually distinguished: qualitative and quantitative. The reliability of qualitative methods, a typical and probably the best known representative of which is the method of targeted interviews (Delphi method) based on a set of targeted and specific questions, is derived from the subjective assessments specified during the evaluation process [5, 16].

On the other side, quantitative methods are, as a rule, based on mathematical formulae expressing risk in the form of numerical values. Thus, results (the estimates of the risk) generated by the quantitative approaches are exact values. It is however important to realize that the problem of subjectivity is only transformed – the values of impacts associated with risks (the numbers) [19] are highly subjective values because the respective formulae are based on empirical assumptions of experts responsible for the risk assessment. This is also why computed results are usually difficult to interpret.

The individual quantitative approaches mutually differ by the complexity of the used formulae [18] and the number of variables appearing in them [11]. Nevertheless, although in different ways, all of them reflect the fact that the mechanism of a risk application

DOI: 10.14736/kyb-2015-3-0408

proceeds in the following manner: a vulnerability makes it possible that a threat overcomes countermeasures and causes harm to an asset. In fact, the asset's price motivates threat activation and the threat elevates the vulnerability. This is why the asset must be protected against threats by implementing countermeasures.

The advantages and disadvantages [1, 11, 12] of the both above mentioned approaches (i. e., quantitative and qualitative) lead us to propose their combination that will be applied in this paper to the design of a complex system evaluating the risk management of information security. The proposed method, like most of other combined approaches, uses semi-qualitative evaluations as input variables and calculation formulae for risk evaluation. The approach is based on a proper uncertain information processing form of implicational rules; their uncertainty [12] is expressed by the grade of vagueness of linguistic terms ("very high", "not so accurate", "nearly" etc.). To formalize this vagueness in lexical constructs, a fuzzy mathematical instrument is used, and the inference mechanisms are based on the principles of fuzzy logic. However, the detailed explanation of these principles is not included in this paper; for this, the reader is referred to [14, 15]. In the described software implementation, fuzzy logical computations are realized with the help of the LFLC 2000 (Linguistic Fuzzy Logic Controller) tool [7].

The main goal of this paper is to describe a model that is a specialization of a general model published in [9]. It is implemented in the comprehensive application shell in the way that several IF-THEN-rule knowledge bases cooperate with the goal to minimize all the shortcomings of usual approaches to risk analysis (and therefore it can be used outside the information security area). Since the model uses the knowledge expressed in vague language, the necessary data does not need to be collected by experts – the identification of assets and their definition is done in vague and common language that is understandable to everybody. Moreover, as it was empirically proved in applications, when used by the experts, the risk analysis is conducted in a surprisingly quick, clear, easy and comprehensive way, with the ability to support the understanding of the processes and results to all of the users.

This paper is organized in a simple and clear way. In the next section we describe the overall structure of the system, while Sections 3 – 6 are devoted to its individual subparts; in these sections, the implementation and realization of the built in processes is described. In Section 7 the reader can find some experimental results.

2. DECISION MAKING MODEL

To make sure that the following description of the system is well understood, let us specify the meaning of the main concepts usually used in the area of information security management [1, 2, 16]:

An **asset** is anything that has a value to the organization that can be depreciated by the exposure to **threats**. By threats we understand potential events, which, when they turn into reality, may cause an undesirable incident and may harm an organization or system. A **vulnerability** is the weakness of an asset (or group of assets) that allows it to be exploited and harmed by one or more threats. The vulnerability is an attribute of an asset and represents the sensitiveness of the asset with respect to the threats.

The concept of **risk** is connected with an event that can occur, with the probability of its occurrence and with its potential impact. It is always future oriented: it relates to

the impact that can appear in the future. To diminish the negative impacts, **protective measures** or **countermeasures** are usually realized. By these terms we understand processes, procedures, technical or legal means or anything else that is designed to mitigate the effect of threats by reducing vulnerability or the impact of threats. Therefore, the threat in our model has two attributes, that are representing the level of the vulnerability of the asset when exposed to the threat and the frequency of threat occurrence.

As stated above, the described decision making model is derived from the general model published in [9]. In fact, it is its specialization for application in the area of information security management [3]. The decision making process from the cited paper is specialized and decomposed into the following six subprocesses (see also Figure 1).

1. Identification of assets with the help of an input questionnaire.
2. Identification of the relevant threats together with their attributes. This is done by a simple expert system on the basis of the assets type and their prices (for more details see below).
3. The risk evaluation is done by a fuzzy expert system that realizes the main part of the decision making process.
4. Design of suitable countermeasures to protect against the identified threats is done by another simple expert system.
5. Most suitable countermeasures reducing risk are selected by another simple expert system. The selection is done with respect to their efficiency and implementation costs.
6. Risk evaluation and the suitable countermeasures are visualized in the customized component model of the system assessed.

The whole model works in the following way: in the first step, the user identifies assets and their attributes (especially price and type, which are described using vague terms from a common language). This means that in the first step the complete description of all the assets (asset price, asset type and dependency – the weight laid on an asset) is set up.

In the second step, relevant threats are assigned to each asset by the first expert system (the set of all threats is stored in its knowledge base).

Subsequently (step 3), using the given inference rules, the risk levels of the individual threats are evaluated. This means that their characteristics "frequency" and "vulnerability" are assigned with the help of the knowledge base. For this, it is necessary to evaluate the respective risk for all the individual threats of all of the individual assets. At this point it may be of interest to note that this will later enable us to select suitable countermeasures restraining the identified threats.

The next subprocess (step 4) conducts the assignment of appropriate countermeasures based on the risk evaluation, asset type and individual threat (as every threat linked in the preceding step to any asset has its own risk level).

The following subprocess (step 5) is the selection of the most suitable countermeasures that reduce the risk to an acceptable level, with respect to their efficiency and implementation price.

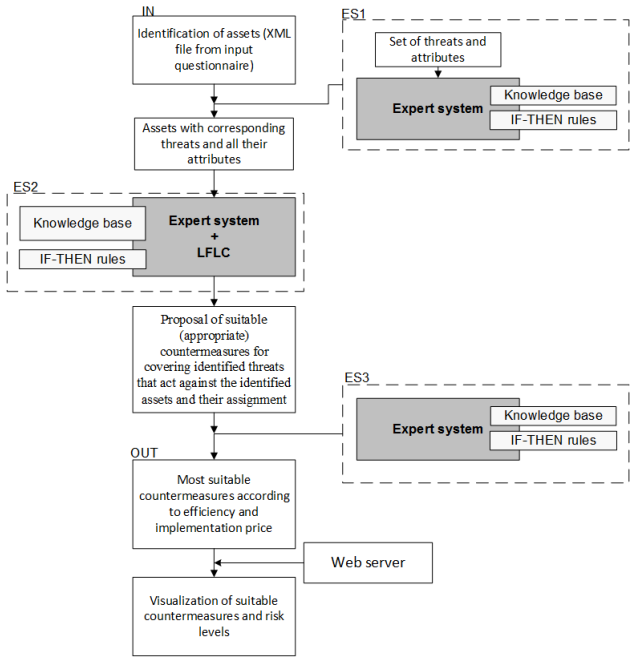

Fig. 1. Structure of the system.

The final subprocess (step 6) presents the risk evaluations and suitable countermeasures in the form of the customized component model [20], where assets are represented by components and countermeasures are represented by subcomponents.

3. IDENTIFICATION OF ASSETS

As said above, the purpose of the first step of the whole process is to identify all the important assets with the help of an input questionnaire. Through this questionnaire, users define the assets that occur in their organization and all the attributes of such assets. An example of such input questionnaire is depicted in the following Figure 2.

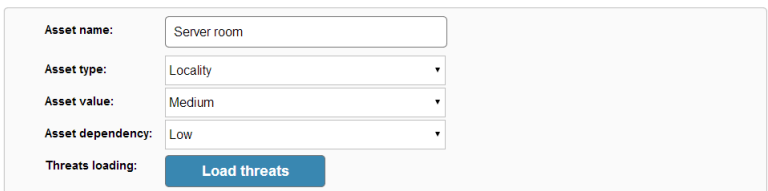

Fig. 2. Asset definition.

The figure shows one identified asset called "Server room". The asset is of "locality" type – in the questionnaire the selection of the asset type is implemented in the way that the user selects an element from the predefined list of asset types (i. e. LAN, Server, Data asset,...). The price of the "Server room" is a fuzzy linguistic value "medium" and represents the vague evaluation of the asset price. Further, the questionnaire contains another fuzzy linguistic variable called dependency. The dependency of the "Server room" asset is identified as "low". The dependency represents the weight laid on a given asset – this enables us to specify the importance of the asset for an organization, to specify whether it is critical or unimportant. There is a button "Load threats" in the input questionnaire that initiate the expert system operation. Thus, the example in Figure 2 reads that the input is the asset server room, which is a locality with medium price and low importance.

We can thus see that the questionnaire includes vague information expressed in a common language, which is defined by linguistic values. Input fuzzy variables are modeled in LFLC 2000 tool [7], an example of which, together with the form of fuzzy sets, can be graphically seen in Figure 3.

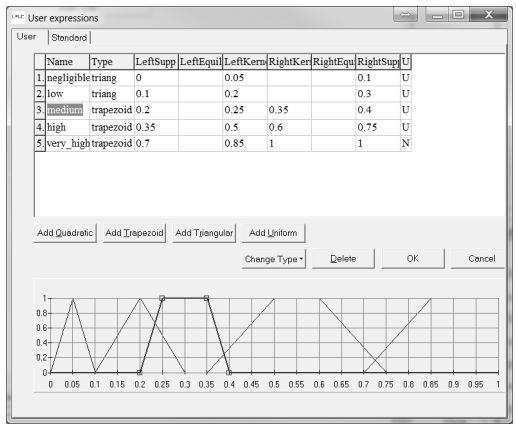

Fig. 3. Fuzzy variable "asset price".

As depicted in Figure 3, the fuzzy sets representing linguistic values may have both triangular and trapezoid forms [10]. These forms of sets, i. e., their kernels (the set where the membership function equals 1) and supports (the set where the membership function is bigger then 0 and lower then 1) were defined by experts in problem domain and fine-tuned during testing.

4. ASSIGNING RELEVANT THREATS

Having obtained records of assets as a result of the activity described in the preceding section, we will in this section now describe how threats are assigned to the individual assets based on their type. The asset records are extended with two characteristics (frequency and vulnerability) – every asset can have, and usually does have, multiple

corresponding threats where every occurrence of any threat comes with one frequency attribute and one vulnerability attribute):

- Vulnerability – fuzzy linguistic variable that defines the level of asset vulnerability in the case of the threat occurrence (values: "very low", "low", "medium", "high", "very high").
- Threat frequency – fuzzy linguistic variable (values: "occasional", "low", "medium", "high", "extraordinary").

This extension of asset records is done by the first simple expert system (see block ES1 in Figure 1) consisting of 108 IF-THEN rules. The form of such rules is: IF asset type THEN Threat(frequency of the threat / vulnerability level)

The threats are brought from the ISO/IEC norms [3], which ensures for instance usability of ISO certifications and implementations, and compliance with Czech cybernetic laws. Let us present a couple of examples of IF-THEN rules for selection relevant threats.

IF asset_type="User access to the IS" THEN {threat="Operation error"(frequency="high", vulnerability="very low")}

IF asset_type="Software" THEN {threat="Unauthorised use of equipment by foreign entities"(frequency="extraordinary", vulnerability="very low")}

IF asset_type="Data storage" THEN {threat="User error"(frequency="low", vulnerability="low")}

For instance, the first rule means, that when asset of "User access to the IS" type is identified, the threat "Operation error" with the frequency attribute "high" and the vulnerability attribute "very low" is selected by the expert system.

5. COMPUTATION OF RISK VALUES

In this step, risks are evaluated with the help of the second set of fuzzy IF-THEN rules. This is realized in the main part of the proposed system formed by the fuzzy expert system (see block ES2 in Figure 1) whose knowledge base consists of 625 IF-THEN rules, examples of which follow:

IF asset_price="low" AND threat (frequency="low", vulnerability="low") AND dependency="low" THEN risk="acceptable"

IF asset_price="low" AND threat (frequency="low", vulnerability="medium") AND dependency="low" THEN risk="acceptable"

IF asset_price="low" AND threat (frequency="low", vulnerability="high") AND dependency="low" THEN risk="acceptable"

IF asset_price="medium" AND threat (frequency="medium", vulnerability="low") AND dependency="low" THEN risk="acceptable"

IF asset_price="medium" AND threat (frequency="medium", vulnerability="medium") AND dependency="medium" THEN risk="very low"

All of these rules were formulated by problem domain experts and were tested on several system prototypes and risk analysis projects. The output of this expert system, i. e. the evaluation of the considered risk, is a value of the linguistic variable "risk" (i. e. "acceptable", "low", "medium", "high"). The rules have the following form: IF asset price AND threat (frequency, vulnerability) AND dependency THEN risk. This expert system is realized in LFLC tool [7, 10].

The fuzzy expert system employed in this step uses CNF (Conjunctive Normal Form) fuzzy approximation as the inference method and the COG (Simple Center of Gravity) as the defuzzyfication method (these were selected after extensive testing) [13, 14]. CNF approximation and COG defuzzyfication are applied by the LFLC for the risk evaluation [7]. The LFLC tries to find IF-THEN rules, that can be applied. Based on the deffuzification method, the LFLC itself selects the most appropriate IF-THEN rule and applies it. The output fuzzy value is therefore either an initial (basic) value (acceptable, low, medium, high) or a composition of some basic value extended by a fuzzy operator [10] (very low, very high).

6. SELECTION OF THE MOST SUITABLE COUNTERMEASURES

The proposal of both possible and most suitable countermeasures is conducted by another expert system (see block ES3 in Figure 1). All identified threats that act against some of the assets must be eliminated. The countermeasures are suggested by another set of fuzzy IF-THEN rules. So, analyzing the vague input information (acquired from the input questionnaire), this expert system assigns relevant countermeasures to individual assets (together with defining their price and effectiveness).

First, the relevant countermeasures are determined. The relevance is detected with the help of two knowledge bases – two sets of IF-THEN rules – one describing the affinity of countermeasures to asset types and second describing the affinity of countermeasures to threats.

As an example, let us present a snippet of one rule from the first knowledge base applicable on the identified asset "switch" (defined as asset of "LAN" type):

IF asset_type="LAN" THEN select COUNTERMEASURES {"Equipment siting and protection"; "Supporting utilities"; "Cabling security"; "Equipment maintenance"; ...; "Documented operating procedures"; "Change management"; "Fault logging"; ...; "Equipment identification in networks"; ...; "Key management"; "Control of technical vulnerabilities"; }

The second set of rules may be illustrated by the following snippet (for threat "Remote spying" that was selected for asset "switch"):

IF threat="Remote spying" THEN select COUNTERMEASURES {"Cabling security"; "Network controls"; ...; "Policy on use of network services"; "User authentication for external connections"; "Equipment identification in networks"; "Key management"; "Control of technical vulnerabilities"; "Reporting information security events"; ... }

The relevant countermeasures are those that are generated by the both considered knowledge bases. The reason for considering only the intersection of results generated by the two expert systems is to provide the relevant and suitable countermeasures as a response to the individual threat and individual asset type (one threat can manifest against multiple assets, which don't share same characteristics – by the application of the intersection, the system will not present countermeasures that are not relevant for the identified individual asset).

Following this, the most appropriate countermeasures are chosen. The knowledge base conducting this selection is again constructed in the LFLC tool. Examples of IF-THEN rules for countermeasures selection (where the attributes price and efficiency are specified in the braces):

IF asset_price="very low" AND risk="low" THEN intersecting_countermeasures WITH (price="low", efficiency="low")

IF asset_price="medium" AND risk="low" THEN intersecting_countermeasures WITH (price="low", efficiency="medium")

IF asset_price="medium" AND risk="medium" THEN intersecting_countermeasures WITH ((price="low", efficiency="high")

The outputs and results of the risk analysis conducted by our set of expert systems is a visualization (step 6) that is using a modified component model [20], where the components represent assets and the subcomponents represent the countermeasures relevant to the assets. The colors of components represent the risk value of the asset and the colors of the subcomponents represent the effectiveness of the selected and proposed countermeasures.

7. COMPARISON AND RESULTS

Let us demonstrate the whole process on a simple example. Naturally, because of the extent of the risk analysis procedure we will use only a snippet of it. The usual approach is that an expert proposes the evaluation criteria (numeric evaluations of assets, threats and their attributes). Then the expert collects information from users, usually in the form of a table [11, 12] – such table contains the necessary attributes that are being used in the formulae for the risk calculation.

Using a classical approach described for instance in [17], the expert identifies an asset and specifies risk which is computed using a simple equation [17]

$$A(x) * T(x) * V(x),$$

where

A is the asset price (from a range of 1–4),
T is the probability of the threat (from a range of 1–5),
V is the value for vulnerability (from a range of 1–5),
x is the particular asset.

As an example consider an asset "switch". The expert tries to identify a set of threats (depending on the time the expert has, his/her expertise and the strategy he/she chooses [11] the set may wary). Respondents of targeted interviews evaluate the price of asset "switch" (let it be in our example the number 2) and in cooperation with the expert they evaluate the values for vulnerability and probability of each identified threat. Let us assume that they identified three threats and their attributes are evaluated as follows:

- *infiltration* with vulnerability value 2 and probability value 2,
- *hardware malfunction* with vulnerability value 1 and probability value 1, and
- *maintenance error* with vulnerability value 1 and probability value 1.

For every threat, the risk value is computed according to the above presented formula. In the considered example the expert gets values – *infiltration* $= 2 * 2 * 2 = 8$; *hardware malfunction* $= 2*1*1 = 2$; *maintenance error* $= 2*1*1 = 2$. Now the expert determines a threshold value (let it be in our example 5) determining that every risk value above this threshold must be covered by countermeasures. After this evaluation, the expert suggests the countermeasures according to his domain knowledge.

To get the corresponding results, our approach uses the terms from a vague common language, so there is no explicit scale of numeric values or need for its approval. Also the collecting of the data for analysis is not provided by experts, but by users using an input questionnaire.

In the first step, the users identify the asset "switch" (asset type "LAN") and assigns to it a price ("medium") and dependency (it is a core switch, so the dependency is "very high").

Following this (in step 2), the system provides all the relevant threats and their corresponding attributes (selecting only the relevant one from the whole knowledge base), the snippet of the relevant threats may be:

"Disturbance" (frequency = "very low"; vulnerability = "medium")
"Breach of maintainability" (frequency = "low"; vulnerability = "low")
"Remore spying" (frequency = "medium"; vulnerability = "medium")
"Theft" (frequency = "occasional"; vulnerability = "medium")
"Dust, corrosion, freezing" (frequency = "occasional"; vulnerability = "very low")

In the third step, the system evaluates risk levels of all the provided threats. It may happen that some of the treats may appear in connection with several assets and with different attributes. This is because, the threats can represent different events (e. g. threat "Theft" can represent theft conducted by the internal staff or theft conducted by an external thief). So, the risk levels of threats corresponding to the identified asset "switch" may be:

"Disturbance" – risk="medium";
"Breach of maintainability" – risk="low";
"Remore spying" – risk="low";
"Theft" – risk="medium";
"Dust, corrosion, freezing" – risk="low";
"Destruction of wiring" – risk="low".

In the considered example of a "switch" asset and the above evaluation, the system proposes countermeasures for the threats and the asset (according to asset type) by the intersection of sets of countermeasures linked to the asset (see Section 6).

The fifth step of the system selects only the most suitable countermeasures. Because not a single risk is evaluated "acceptable", the system is processing all the threats from the previous step. Because of the asset price being "medium" and not a single risk being more than "medium", the system excludes all the countermeasures with price "high" and all countermeasures with "low" efficiency regardless of their price. The snippet of the final list of recommended countermeasures may be like this:

"Equipment siting and protection" (price="small", efficiency="big")
"Supporting utilities" (price="small", efficiency="big")
"Cabling security" (price="small", efficiency="big")
"Equipment maintenance" (price="small", efficiency="big")
"Network controls" (price="small", efficiency="big")
"Security of network services" (price="small", efficiency="medium")
"Monitoring system use" (price="small", efficiency="big")
"Segregation in networks" (price="small", efficiency="big")
"Network connection control" (price="small", efficiency="big")
"Network routing control" (price="small", efficiency="big")
"Key management" (price="small", efficiency="big")
"Control of technical vulnerabilities" (price="small", efficiency="big")

8. CONCLUSION

The presented paper deals with application of a model for decision-making under uncertainty for implementation of complex software tools, such as information security risk management – the tool is published at the web URL `http://ar.proit.cz`. The results have shown that the model proposed in [9] is suitable for these tasks. The experience gained are reflected retroactively to the expert systems rules. The expert on information security risk analysis is no longer necessary to perform the analysis. The results are implemented in fully matured applications, that are ready for usage in the problem domain. The decision making model itself is very versatile and can be used in other domains – today, the problem domain of searching over dynamic and static content and the problem domain of operation system designs are being implemented.

(Received March 19, 2014)

REFERENCES

[1] ČSN ISO/IEC TR 13335-3: Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security. Český normalizační institut, Praha 1999, pp. 1–25.

[2] ČSN ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements. Český normalizační institut, Praha 2006, Annex A.

[3] J. Bartoš, J. Procházka, C. Klimeš, B. Walek, and M. Pešl: Fuzzy reasoning model for decision making under uncertainty. In: 16th International Conference on Soft Computing Mendel 2010, Brno 2010.

[4] J. Bartoš, J. Procházka, C. Klimeš, B. Walek, and M. Pešl: Fuzzy reasoning model for decision making under uncertainty. In: 16th International Conference on Soft Computing Mendel 2011. Brno 2010, pp. 203–209.

[5] J. Bartoš and B. Walek: A methodology for testing of information system under uncertainty. In: Proc. 36th International Conference on Telecommunications and Signal Processing (TSP), Faculty of Electrical Engineering and Communication, Brno University of Technology, Brno 2013, pp. 20–22. DOI:10.1109/tsp.2013.6613883

[6] J. Bartoš, B. Walek, P. Smolka, J. Procházka, and C. Klimeš: Fuzzy modeling tools for information system testing. In: 17th International Conference on Soft Computing Mendel 2011. Brno 2011, pp. 154–161.

[7] H. Habiballa, V. Novák, A. Dvořák, and V. Pavliska: Using software package LFLC 2000. In: 2nd International Conference Aplimat, Bratislava 2003, pp. 355–358.

[8] C. Klimeš and J. Procházka: Reasoning in Software Support and Maintenance. In: Abstracts of Contributions to 5th International Workshop on Data–Algorithm–Decision Making. DAR – UTIA 2009/3, Praha 2009.

[9] C. Klimeš: Expert System Utilization for Modeling the Decision Making Processes upon Indetermination. Acta Electrotechnica et Informatica *1* (2007), 1.

[10] C. Klimeš and J. Procházka: Research paper: Using LFLC for decision making in SW support and maintenance. In: Research intention DAR – OASA 2/2009. Ostrava 2009.

[11] R. L. Krutz and R. D. Vines: The CISSP Prep Guide–Mastering the Ten Domains of Computer Security. John Wiley Sons, Inc., 2001, pp. 12-33.

[12] M. Makowski: Mathematical Modeling for Coping with Uncertainty and Risk. In: System and Human Science for Safety, Security and Dependability, November 2003, pp. 1–20. DOI:10.1016/b978-044451813-2/50004-x

[13] V. Novák: Fuzzy množiny a jejich aplikace. SNTL, Praha 1986.

[14] V. Novák: Fuzzy Relation Equations with Words. First edition. Springer,Heidelberg 2004, pp. 167–185. DOI:10.1007/978-3-540-39675-8_6

[15] V. Novák, I. Perfilieva, and J. Močkoř: Mathematical Principles of Fuzzy Logic. First edition. Kluwer Academic Publishers, Boston – Dordrecht – London 1999. DOI:10.1007/978-1-4615-5217-8

[16] B. Walek, J. Bartoš, and J. Žáček: Proposal of The Expert System for Conducting Information Security Risk Analysis, Proceedings of the International Conference on Electrical and Electronics Engineering, Clean Energy and Green Computing. In: The Society of Digital Information and Wireless Communications, 2013, pp. 58-68.

[17] F. Steiner and J. Tupá: Management rizik v systémech řízení bezpečnosti informací. In: MOPP 2007. Západočeská univerzita, Plzeň 2007, pp. 177–183.

[18] H. Šegudović: Quantitative risk analysis method comparison. In: MIPRO 2007 conference, ISS, pp. 1–6.

[19] H. Šegudović: Upravljanje sigurnošću informacijskih sustava. In: KOM 2003, FER LSS, 2003, pp. III 31–40.

[20] B. Walek, J. Bartoš, and C. Klimeš: A methodology for creating a conceptual model under uncertainty. In: International Conference on Computer, Electrical, and Systems Science, and Engineering, Amsterdam 2012, pp. 86–92.

Cyril Klimeš, Ústav informatiky, Mendelova univerzita v Brně, Zemědělská 1, Brno. Czech Republic.
e-mail: cyril.klimes@mendelu.cz

Jiří Bartoš, Královéhradecká 484, Ústí nad Orlicí. Czech Republic.
e-mail: jiri.bartos@viavis.cz