ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
UDC/UDK 004.773.3.056:159.9.019.4]:004.822

AN APPROACH TO THE ASSESSMENT OF POTENTIALLY RISKY BEHAVIOR OF ICT SYSTEMS' USERS

Krešimir Šolić, Franjo Jović, Damir Blažević

Preliminary notes

Information and Communication Technology system's user should be considered as system's component, because user's behaviour can significantly affect the system's security level. The aim of this paper is to develop an assessment method for user's potentially risky behaviour. Ontology and OWL symbolic language have been chosen in order to define the semantic model and to formalize the knowledge of the domain on "user's potentially risky behaviour". The Evidential Reasoning algorithm has been chosen for assessment of user's behaviour. The normalized results for assessment on user's behaviour give an interval ranging from 0,066 for the "naïve" user to 1,000 for the "paranoid" system's user which can be used for reference in future work. This paper shows how to use the Evidential Reasoning algorithm to evaluate the human part of a technical system, how to evaluate a group of users instead of an individual evaluation. Furthermore, conditions required to map the algorithm to the ontological structure are defined.

Keywords: *e-mail, evidential reasoning, ICT system, ontology, security, user's behaviour*

Metoda procjene stanja mogućeg riskantnog ponašanja korisnika IKT sustava

Prethodno priopćenje

Korisnika informacijsko-komunikacijskog sustava treba promatrati njegovim sastavnim dijelom, jer korisnik svojim rizičnim ponašanjem može značajno utjecati na ukupnu razinu sigurnosti sustava. Cilj rada je razviti postupak modeliranja sustava za procjenu rizičnog ponašanja korisnika. Ontologija i OWL simbolički jezik su odabrani za izradu strukture semantičkog modela odnosno formalizaciju prikupljenog znanja iz domene "ponašanja korisnika sustava sa stajališta sigurnosti". Za procjenu ponašanja odabran je algoritam za evidencijsko zaključivanje koji se koristi za pocjenu stanja te omogućuje usporedbu zatečenog stanja više sustava. Dobiveni normirani rezultati obrade su dali ocjenu ponašanja korisnika u rasponu od 0,066 za naivno do 1,000 za "paranoidno" ponašanje. U radu je prikazan način upotrebe algoritma za evidencijsko zaključivanje prilikom procjene ljudskog dijela tehničkog sustava, način procjene cijele grupe umjesto pojedinačnog procjenjivanja te su definirani uvjeti mapiranja algoritma i ontološke strukture.

Ključne riječi: *e-mail, evidencijsko zaključivanje, IKT sustav, ontologija, ponašanje korisnika, sigurnost*

1 Introduction and problem statement

The role of users' behaviour should be acknowledged when developing different information security solutions [1], because users of the ICT system can significantly compromise the security of that system [2, 3]. In this paper a model for assessment of users' behaviour regarding security issues is proposed. The model is applied to the e-mail subsystem as part of the ICT system.

The e-mail service has been chosen because it is widely accepted and frequently used for both personal and professional communication, due to its accessibility and ease of usage. On the other hand e-mail is a communication channel that is mostly corrupted by malicious attacks (spam, viruses, increased direct attacks, etc.) during the last few years [4].

According to statistics, majority of security breaches in professional organizations are caused by insiders not always with malicious intent [5]. Because of that, special attention should be paid to the e-mail system and all the employees should have basic understanding of the ICT security issues [5].

In order to formalize user's risky behaviour the application of ontology can be considered as the most promising knowledge formalization tool. It entails a comprehensive approach to the information security policy. The W3C's Web Ontology Language (OWL) is regarded as the most promising ontology language in the past five years [6].

The aim of this paper is to build ontology on the user's potentially risky behaviour regarding security of the e-mail system by using Protégé – OWL tool [7]. Thus formalized knowledge becomes reusable and maintainable for other domain experts and can also be relatively easily extended or integrated within similar ontology.

Users' behaviour data was collected by a specially designed questionnaire based on the developed OWL ontology. Conditions were defined for mapping the Evidential Reasoning (ER) algorithm on the ontology hierarchical structure in order to define the method for the assessment of users' risky behaviour. Moreover, a normalized grade interval was defined by simulating a "naïve" and a "paranoid" user and several individuals were interviewed in order to present the usage of the proposed method.

2 Formalizing knowledge

Ontology is used to formally define knowledge about some domain of interest by defining concepts and relations between them [8, 9].

2.1 Defining domain of user's risky behavior

The basic elements of ontology on user's risky behaviour and possible security issues regarding usage of the e-mail system [10] are presented:

- Using unprotected PC;
- Using less secure web browser or its older version;
- Not encrypting sensitive e-mails;
- Using web-browser when secure e-mail client is available;
- Opening problematic attachments (executable, from unknown senders);
- Not being critical/cautious to the unknown senders;

- Replying to strange/fake e-mails (phishing);
- Sending personal and sensitive data by e-mail;
- Forwarding chain letters with list of all e-mail addresses included;
- Registering on questionable web sites;
- Leaving e-mail addresses to be publicly known;
- Taking no care for authentication data (e.g. revealing them to the friend in need);
- Using a less secure e-mail service provider.

Different guidelines and information security policies explain in detail how to make an ICT system more secure. E-mail security technology mostly concentrates on technical details, but they are beyond typical user's reach [11].

Even a project that tries to build overall ontology about ICT security issues in the sub-ontology about users cover only their basic information, but fail to cover user's behaviour data [12]. Because building ontology is an iterative process, basic methodology and guidelines for future work on the ontology of ICT system user's risky behaviour is proposed.

2.2 Ontology structure of the user's behaviour

Expert systems have recently recognized three knowledge types and make a clear distinction between them (even in the philosophical domain) by imposing distinct formalization means and distinct usage routines [13]:

- descriptive knowledge
- procedural knowledge
- factual knowledge

Descriptive knowledge (also referred to as conceptual knowledge) describes the domain concept and the relations among concepts. In that way, every concept is described by defining its relation to the other previously defined concepts. *Procedural* or actionable knowledge describes the procedures and actions that should be taken in given situations. The third type of knowledge recognized in the expert systems is *factual* knowledge that refers to formalization of facts describing the given situation.

This paper focuses on the descriptive knowledge type as the basis for this work, but it is possible to incorporate other two types of knowledge in the proposed ontology as well.

Ontology consists of classes, properties (also known as slots) and individuals (or instances) and its structure depends on formal versions: the Frames-based version or the OWL-based version of ontology [7, 8, 14].

Frames-based ontology is usually written using Resource Description Framework (RDF) files based on Extensible Markup Language (XML). It is an old and simpler framework but still widely used. OWL is one of the mostly used standard ontology languages written in the XML format and is considered as a semantic upgrade of the RDF [14].

Even though both versions of ontology can be used in this model, OWL ontology has been chosen because it is more frequently used nowadays and provides better features for reuse and possible upgrades in future work [6, 8, 14, 15].

There are three types of OWL sublanguages differentiated by their expressiveness: OWL Lite, OWL DL and OWL Full. OWL DL has been chosen for this work because it is the most commonly used and recommended sublanguage [8, 16].

As main building blocks, OWL classes are interpreted as sets that contain individuals (objects in the domain of interest). They are described using formal logical descriptions that state precisely the requirements for membership of the class. Classes are organized into a superclass-subclass hierarchical taxonomy. The word *concept* is sometimes used instead of class. The class *Thing* as main and default class of all ontology is the class that represents the set containing all individuals and all classes [8]. One possible structure of classes for user's risky behaviour could be as follows:

- Thing
  - UsersBehavior
    - UsageOfEmailAddress
      - WayOfUsage
      - UsageOfFreeSystem
        - WayOfUsage
      - RegistrationOnInternet
        - KindOfAddress
      - LeavingAddressOnInternet
        - KindOfAddress
    - TheWayOfAccess
      - ViaWebBrowser
        - PlaceOfAccess
      - ViaEmailClient
      - ViaProtectedPC
    - AttitudeTowardCollocutor
      - Criticism
      - OpeningAttachments
    - UsageOfSystem
      - UsageOfEncryption
      - SendingPersonalData
      - ForwardingMassEmails
      - LoggingOutOfSystem
    - QualityOfPassword
      - PasswordSelfAssessment
      - PasswordReUsage
      - PasswordRecorded
        - PlaceOfRecord
      - PasswordBorrowed

Properties are binary relations linked to individuals. Properties are roughly equivalent to slots in frame ontology, also known as roles in description logics, and as relations in Unified Modeling Language (UML) and in other object-oriented notions. There are two main types of properties, Object properties and Datatype properties. OWL also possesses a third type of property known as Annotation property that can be used to add metadata [8]. Object properties in user's behaviour ontology are as follows:

- topObjectProperty
  - hasAddress

  - usesOnTheWay
  - usesFreeSystems
    - usesOnTheWay
  - usesForRegistration
    - usesKindOfAddress
  - leavesOnInternet
    - usesKindOfAddress
- usesAccess
  - usesWebBrowser
    - hasAccessingPlace
  - usesEmalClient
  - hasProtectedPC
- hasCollocutor
  - hasCriticism
  - opensAttachments
- usesSystem
  - usesEncryption
  - sendsPersonalData
  - forwardsMassEmail
  - logesOut
- hasPassword
  - hasAssesment
  - hasMore
  - isRecorded
    - hasPlace
  - isBorrowed

Datatype and Annotation properties are not defined as they are not necessary for this model.

Instances are defined as grades ranging from one to five, meaning from poor to excellent. Some classes can possess all of the instances as a value, and some classes can only have two or three instance values regarding the object presented.

In this model the class "UsersBehavior" and the subclass "UsageOfEmailAddress" possess all five possible instances, because they can have all five possible grades while the subclass "WayOfUsage" possesses only two instances: poor and excellent.

The ontology graph with classes, sub-classes, properties and instances defined in Protégé – OWL editor tool is shown in Fig. 1.

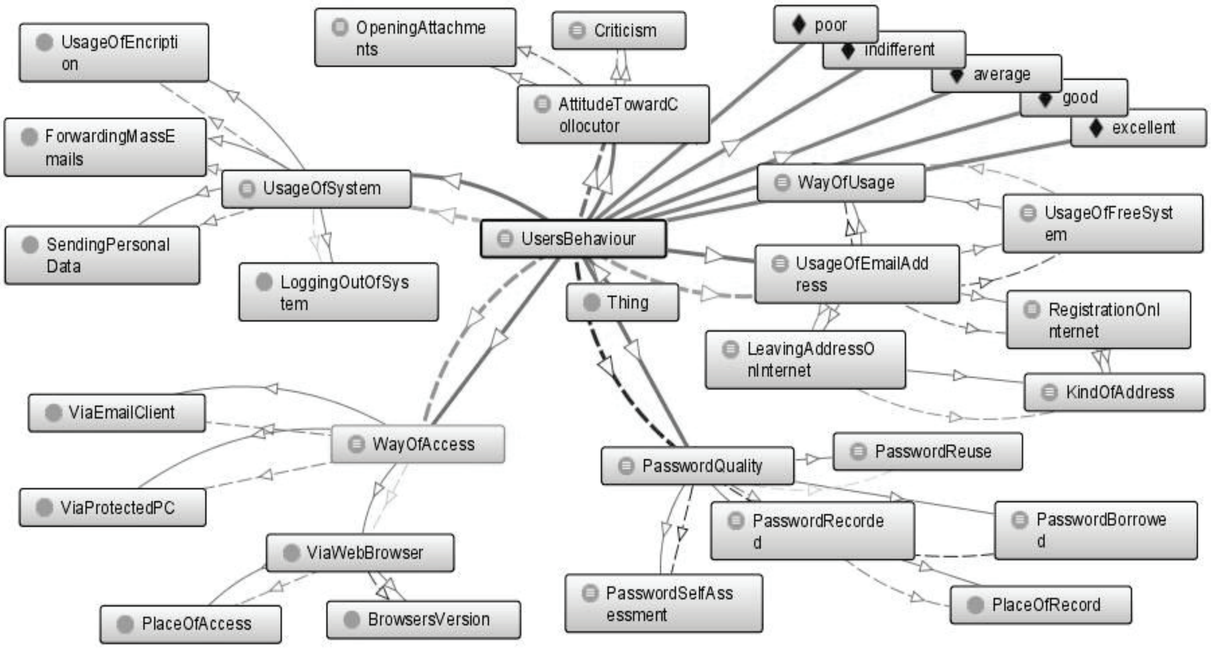

Figure 1 Formaly defined domain of knowledge in ontology editor Protégé 4.1

3 Assessment algorithm of ICT user's risk

According to the proposed model, the user is assumed to be a constitutive part of the ICT system. The risk of system use on user's part can be modelled as a part of a risk chain [17] on the premises of risk equation that connects ICT throughput, ICT resource and system risk that is inherent for all non-growth, non-evolving, agent-directed systems [18].

The ER algorithm that is chosen for risk modelling includes a hierarchical model of human and organizational error taxonomy similar to Grabowski model [17]. It allows multiple questionnaire answers thus enabling a particular user that did not answer one or more questions to be graded as well. The missing data are taken as uncertainty. The impact of non-uniform user's risky behaviour is expressible as weighting attributes of different system parts in the total ER calculation.

Some examples of the ER algorithm application to technical systems are: the oil reserve forecast [19], motorcycle evaluation [20], car industry [21], expert system [22], knowledge reduction [23], risk analysis [24] and electric power grid [25].

3.1 Description of ER algorithm

The evaluation grades are stated as poor, indifferent, average, good and excellent. In order to perform the assessment, at least a two level hierarchy in ontology is needed such as *superclass-subclass hierarchy*. High-level attributes are assessed through associated lower level attributes in the hierarchical assessment. The uncertain judgments are allowed in case of indeterminism of a certain attribute.

For example if the user gives more answers or no answer in the question about self-assessment of password quality grades would be as follows:

- The sum of grades would contain 50 % of grade *average* and 50 % of grade *excellent*, for the case where the user gives two answers;
- The grade would be 100 % *average*, if the user gives one particular answer;
- The sum of grades would contain 50 % of grade *poor* and 30 % of grade *good*, if the answer was "I do not know";
- The value 0 % for all grades would be if the user gave no answer.

The percentages in the above assessments are referred to as degrees of belief and may be used in decimal format as 0,3; 0,5 and 1. Degree of belief equal to 100 %, for one particular answer, represents "absolutely sure" belief. The third assessment is incomplete as the total degree of belief is 0,8, while the first and second assessments are complete. The missing value of 0,2 in the third assessment represents the degree of ignorance or uncertainty. The fourth assessment is a special case and it presents total ignorance or 100 % of uncertainty.

It is possible to define the proportion of grades as degrees of belief in order to perform assessment on the whole group of users. For example, the basic group attribute of password self-assessment would be distribution of proportions on how many users grade their password with particular evaluation grade. One distribution of grades under group of users could be:

S (password self-assessment) = {(poor, 0,19), (average, 0,43), (excellent, 0,32), (uncertainty, 0,06)}. (1)

In this example 32 % of users answered as excellent, 43 % as average, 19 % as poor and 6 % did not know how to self-assess their password or did not answer that question.

The problem is how to generate an overall assessment of password quality by aggregating the above possible judgments in a rational way. The ER approach [26, 27] is a suitable method for dealing with the aggregation problem.

3.2 ER algorithm and its enhancement

The ER algorithm is well suited for dealing with a multiple-criteria decision analysis (MCDA) problem which considers quantitative and qualitative measurements assessed using subjective judgments with uncertainties. This approach was introduced in the 1990s [28, 29] and is based on the Dempster-Shafer (D-S) theory [30, 31], the decision-making theory [32] and the evaluation analysis model [33].

In order to use the ER algorithm to aggregate attributes of a multilevel structure, certain enhancement was done with four proposed synthesis axioms [28]:

- If no basic attribute is assessed to an evaluation grade at all, then the general attribute should not be assessed to the same grade either.
- If all basic attributes are precisely assessed to an individual grade, then the general attribute should also be precisely assessed to the same grade.
- If all basic attributes are completely assessed to a subset of grades, then the general attribute should be completely assessed to the same subset as well.
- If any basic assessment is incomplete, then a general assessment obtained by aggregating the incomplete and complete basic assessment should also be incomplete with the degree of incompleteness properly assigned.

The use of utility and utility interval gives a single numerical value as the overall grade of user's risky behaviour thus enabling a comparison between different users or groups of users [20, 34]. A detailed explanation of the Enhanced ER algorithm can be found in [20].

Calculations were done by the System assessor software that was previously developed by the authors [34]. There is also a possibility to use the commercial software package the Intelligent Decision System (IDS) tool [35].

4 Assessment of users' risky behaviour

In order to apply the ER algorithm on the *superclass-subclass hierarchical* structure defined in ontology some conditions have to be met:

- Hierarchical structure should be an acyclic graph;
- Every direct relation should be "one-to-one" or "one-to-many";
- Crossing between classes should be reorganized.

If these conditions are not met in the ontology, one solution would be to add additional classes in ontology in order to satisfy the acyclic property and to reuse some lower level classes by repeating them with same grades and same degrees of belief in order to reorganize "many-to-many" relationship.

In the ontology structure every smallest subclass has a matching question in the questionnaire and for each instance of that subclass defined in ontology there were possible answers. These subclasses present attributes in the *ER hierarchical structure*. The first question was regarding subclass "WayOfUsage" with possible answers "yes" and "no" that present instances "excellent" and "poor". The instances defined in ontology present grades of attributes in the *ER hierarchical structure* (Tab.1).

Complete questionnaires are obtained by examining ten co-workers in the assessment process and presented for method illustration. The distribution of grades for each basic attribute is calculated from proportion of grades given to each user. The result of the performed assessment across group of users with the aggregation process is presented in Tab. 2.

The comparison of assessment grades distributions and utility numbers between group of users and the "naïve" and the "paranoid" user is shown in Tab. 3.

In this way normalized grades define the interval between "naïve" and "paranoid" (from 0,066 to 1,000) user and the assessment grade on the tested group of users can be interpreted as relatively secure behaviour of the whole group.

Table 1 Matching between answers (basic attributes) and grades (instances)

Basic attributes	Subject of question	Possible answers	Possible grades
WayOfUsage	Differentiation of an address on professional and private	NO YES	P E
UsageOfFreeSystem	Usage of free e-mail systems and in what manner	NO YES a) for professional usage b) personal c) occasional	I A G E
RegistrationOnInternet	Registration on all sort of Internet services and with what kind of e-mail address, mostly	NO YES a) professional b) personal c) occasional	P A G E
LeavingAddressOnInternet	Leaving e-mail address readable/visible/accessible	YES a) professional personal b) occasional NO	P I A E
ViaWebBrowser	Usage of web browser for e-mail service and from what kind of PC	YES/occasionally a) public places (e.g. Internet cafe) b) only from home or office NO	P I A G E
ViaEmailClient	Usage of e-mail client, software tool	NO Mostly YES	I G E
ViaProtectedPC	Taking care of PC's protection (antivirus, upgrades...)	NO YES	P E
Criticism	Critical attitude towards new collocutor	NO YES	P E
OpeningAttachments	Opening attachments sent by unknown collocutor	YES Sometimes NO	P I E
UsageOfEncription	Usage of encryption in e-mail communication	NO/don't know* occasionally YES	I G E
SendingPersonalData	Sending personal data via e-mail (e.g. social security number)	YES/don't know* on an exceptional bases NO	P G E
ForwardingMassEmails	Forwarding mass e-mails, known as "chain-letter"	YES/don't know* Occasionally NO	I G E
LoggingOutOfSystem	Logging out from system at the end of its usage	/NO/don't know* mostly YES	P A E
PasswordSelfAssessment	Assessment of own password	a) bad b) average c) good d) don't know*	P A E
PasswordReUsage	Usage of the same password for most systems	YES NO	I E
PasswordRecorded	Password has been written down but where/how	YES NO …. and place stated	P I A G E
PasswordBorrowed	Borrowing of password, ever	YES NO	P E

* Answer "don't know" was interpreted as YES or NO depending on the question

This normalized interval of grades can be used as a referent interval in future security assessments. Also, with more simulations and testing it is necessary to define a referent value for security average behaviour and sufficiently secured behaviour.

The utility interval was not calculated for these three assessments because the degree of uncertainty in assessment was equal to zero.

5 Discussion and conclusions

The ICT system's user, as its component, can significantly affect security issues of the system. However, user's behaviour is rarely taken into consideration in many different security solutions.

This paper proposes a model for assessment of user's potentially risky behaviour while using e-mail service, in order to evaluate its implication on overall security level of a system.

OWL-ontology was used in order to formally define knowledge domain regarding "user's potentially risky behaviour". Furthermore, assessment model was defined by using the Evidential Reasoning algorithm for calculating the overall grade for a group of users or a single user. Also, a questionnaire based on ontology was developed for data gathering.

The ontology with its properties between classes gives a logical hierarchical structure needed for ER algorithm to be applied to the gathered information. Furthermore, ontology offers the possibility of upgrade and modification to this model depending on the particular case of the application of assessment model.

In this approach the ER algorithm has proven its applicability on evaluation of user's and users' behaviour. It is possible to rank potentially risky behaviour by using utility numbers and normalized interval between "naïve" and "paranoid user's behaviour".

Some model limitations arise from restrictions needed in order to map ontology superclass-subclass structure into ER hierarchal structure. Even though ontology allows multiple parents, cyclic relationships and cross-sections between classes; these properties are not allowed in the hierarchical structure for this evaluation algorithm. Authors' suggestion is to build additional classes in ontology, even duplicate if necessary to meet these restrictions.

Also, it is a rather poor definition of the domain on the user's risky behaviour, because there is little focus placed on this area from the technicians' perspective. However, one of ontology's properties is its simplicity of upgrade which allows simple upgrades of the model and reuse in different areas.

In future work, it should be possible to collect specific data from users regarding their gender, age, professional qualification, working position and assumed general technical knowledge by using additional questions in the developed questionnaire. Accordingly, it should be possible to group users into categories and rank their potentially risky behaviour by applying a normalized interval.

By following the presented modelling procedure, it should be possible to develop a model for assessment on the overall ICT system regarding its security, maintenance or cost effectiveness.

Table 2 Preparation of grades across group of users and assessment process of groups' behaviour

Grades of the general attributes		Grades of basic group attributes	First	Second	Third	Forth	Fifth	Sixth	Seventh	Eight	Ninth	Tenth
UsersBehaviour P(0,074) I(0,135) A(0,066) G(0,050) E(0,672)	UsageOfEmailAddress P(0,092) I(0,115) A(0,275) G(0,117) E(0,398)	WayOfUsage P(0,3) E(0,7)	E	P	E	E	E	E	E	P	E	P
		UsageOfFreeSystem I(0,1) A(0,5) G(0,3) E(0,1)	E	G	A	A	A	G	A	A	G	I
		RegistrationOnInternet A(0,5) G(0,2) E(0,3)	A	G	A	E	A	A	E	A	G	E
		LeavingAddressOnInternet P(0,1) I(0,4) A(0,1) E(0,4)	E	P	E	I	I	E	I	I	A	E
	TheWayOfAccess P(0,224) I(0,369) A(0,029) E(0,376)	ViaWebBrowser P(0,3) I(0,5) A(0,1) E(0,1)	P	A	I	I	I	E	I	P	P	I
		ViaEmailClient I(0,6) E(0,4)	E	E	I	I	I	E	I	I	E	I
		ViaProtectedPC P(0,4) E(0,6)	E	P	E	P	P	E	E	E	P	E
	AttitudeTowardCollocutor P(0,035) I(0,035) E(0,928)	Criticism P(0,1) E(0,9)	E	E	E	E	E	E	P	E	E	E
		OpeningAttachments I(0,1) E(0,9)	E	E	E	I	E	E	E	E	E	E
	UsageOfSystem P(0,088) I(0,184) G(0,187) E(0,539)	UsageOfEncription I(0,5) G(0,3) E(0,2)	G	I	I	E	I	I	I	G	E	G
		SendingPersonalData P(0,3) G(0,4) E(0,3)	G	G	G	P	P	E	E	P	G	E
		ForwardingMassEmails I(0,3) G(0,1) E(0,6)	E	E	E	I	I	G	E	I	E	E
		LoggingOutOfSystem P(0,1) E(0,9)	E	E	E	E	E	P	E	E	E	E
	QualityOfPassword I(0,074) A(0,095) E(0,830)	PasswordSelfAssessment A(0,4) E(0,6)	E	E	E	A	A	A	E	E	A	E
		PasswordReUsage I(0,4) E(0,6)	E	I	E	E	I	E	E	I	E	I
		PasswordRecorded A(0,1) E(0,9)	A	E	E	E	E	E	E	E	E	E
		PasswordBorrowed E (1)	E	E	E	E	E	E	E	E	E	E

Table 3 Comparing assessment results between "naïve" user, group of users and "paranoid" user

	Naive user	Group of users	Paranoid user
Poor	0,810	0,074	0
Indifferent	0,190	0,135	0
Average	0	0,066	0
Good	0	0,050	0
Excellent	0	0,672	1,000
Uncertainty	0	0	0
Utility	0,066	0,799	1,000

6 References

[1] Johnson M. E.; Pfleger S. L. The Human Side of Risk Management // IEEE Security & Privacy, 9, 1(2011), p. 51.

[2] Lukasik, S. J. Protecting Users of the Cyber Commons. // Communications of the ACM. 54, 9(2011), pp. 54-61.

[3] Solic, K.; Sebo, D.; Jovic, F.; Ilakovac, V. Possible Decrease of Spam in the Email Communication. // IEEE MIPRO / Cisic, D.; Hutinski, Z.; Baranovic, M.; Mauher, M.; Ordanic, L. 2011. pp. 170-173.

[4] State of Spam & Phishing - A Montly Report. Symantec. 2010. URL: http://www.symantec.com/content/en/us/enterprise/other_resources/b-state_of_spam_and_phishing_report_12-2010.en-us.pdf (14/12/2011).

[5] IT Security Guidelines. Federal Office for Information Security, Bonn, Germany. 2007. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf (14/12/2011).

[6] Klaic, A.; Hadjina, N. Methods and Tools for the Development of Information Security Policy – A Comparative Literature Review // IEEE MIPRO / Cisic, D.; Hutinski, Z.; Baranovic, M.; Mauher, M.; Ordanic, L. 2011. pp. 190-195.

[7] Protégé software. Stanford Center for Biomedical Informatics Research. URL: http://protege.stanford.edu (14/12/2011).

[8] Horridge, M. A Practical Guide To Building OWL Ontologies Using Protege 4 and CO-ODE Tools. // The University of Manchester. 2011. URL: http://owl.cs.manchester.ac.uk/tutorials/protegeowltutorial/resources/ProtegeOWLTutorialP4_v1_3.pdf (14/12/2011).

[9] Noy, N. F.; McGuinness D.L. Ontology Development 101: A Guide to Creating Your First Ontology // Stanford University. 2001. URL: http://www-ksl.stanford.edu/people/dlm/papers/ontology-tutorial-noy-mcguinness-abstract.html (14/12/2011).

[10] Solic, K.; Grgic, K.; Galic, D. A Comparative Study of the Security Level among Different Kind of E-mail Services – Pilot Study. // Tehnicki vjesnik-Technical Gazette. 17, 4(2010), pp. 489-492.

[11] 650-156: Cisco IronPort Certified Security Professional Exam – Email Security. // IronPort Systems Inc. 2011. URL:http://training.ironport.com/ICSP.html (14.12.2011.).

[12] Fenz, S.; Ekelhart, A. Formalizing Information Security Knowledge. // ASIACCS / Mu, Y.; Ogunbona, P. 2009, pp. 183-194.

[13] Prcela, M.; Gamberger, D.; Jovic, A. Semantic web ontology utilization for heart failure expert system design // MIE / Andersen, S. K. et al., 2008, pp. 851-856.

[14] Jovic, A.; Prcela, M.; Gamberger, D. Ontologies in Medical Knowledge Representation // IEEE ITI / Luzar - Stiffler, V.; Hljuz Dobric, V. 2007, pp. 535-540.

[15] OWL Web Ontology Language Guide. W3C. URL: http://www.w3.org/TR/owl-guide/ (14/12/2011).

[16] OWL Web Ontology Language Overview. W3C. URL: http://www.w3.org/TR/owl-features/ (14/12/2011).

[17] Grabowski, M.; Merrick, J. R. W.; Harrald, J. R.; Mazzuchi T. A.; Van Dorp, R. Risk Modeling in Distributed, Large-Scale Systems. // IEEE Trans. On Systems, Man, and Cybernetics - Part A: Systems and Humans. 30, 6(2000), pp. 651-660.

[18] Bradley, J. A Risk Hypothesis and Risk Measures for Throughput Capacity in Systems. // IEEE Trans. On Systems, Man, and Cybernetics - Part A: Systems and Humans. 32, 5(2002), pp. 549-559.

[19] Zhang, X. D.; Zhao, H.; Wei S. Z. Research on Subjective and objective evidence fusion method in oil reserve forecast. // J Syst Simul. 17, 10(2005), pp. 2537–2540.

[20] Yang, J. B.; Xu, D. L. On the evidential Reasoning Algorithm for Multiple Attribute Decision Analysis Under Uncertainty. // IEEE Transactions on Systems, Man, and Cybernetics - part A: Systems and Humans. 32, 3(2002), pp. 289-304.

[21] Liu, X.B.; Zhou, M.; Yang, J.B.; Yang, S.L. Assessment of strategic R&D projects for car manufacturers based on the evidential reasoning approach. // Int J Comput Intell Syst. 1(2008), pp. 24–49.

[22] Beynon, M.; Cosker, D.; Marshall, D. An expert system for multi-criteria decision making using Dempster–Shafer theory. // Expert Syst Appl. 20(2001), pp. 357–367.

[23] Wu, W. Z.; Zhang, M.; Li, H. Z.; Mi, J. S. Knowledge reduction in random information systems via Dempster–Shafer theory of evidence. // Inf Sci. 174, 3,4(2005), pp. 143–164.

[24] Srivastava, R.P.; Liu, L. Applications of belief functions in business decisions: a review. // Inf Syst Frontiers. 5, 4(2003), pp. 359–378.

[25] Jovic, F.; Filipovic M.: Blazevic D.; Slavek, N. Condition Based Maintenance in Distributed Production Environment. // Machine engineering. 4, 1,2(2004), p. 180-192.

[26] Buchanan, B. G.; Shortliffe, E. H. Rule – Based Expert Systems, Reading. Addison-Wesley Publishing Company, Massachusetts, 1984.

[27] Yager, R. R. On the Dempster-Shafer framework and new combination rules. // Inf. Sci. 41, 2(1995), p. 317-323.

[28] Yang, J.B.; Singh, M.G. An evidential reasoning approach for multiple attribute decision making with uncertainty. // IEEE Trans Syst Man Cybern. 24, 1(1994), pp. 1–18.

[29] Yang, J. B.; Sen, P. A general multi-level evaluation process for hybrid MADM with uncertainty. // IEEE Trans Syst Man Cybern. 24, 10(1994), pp. 1458–1473.

[30] Dempster, A. P. Upper and lower probabilities induced by a multivalued mapping. // Ann Math Stat. 38(1967), pp. 325–339.

[31] Shafer, G. A mathematical theory of evidence. Princeton University Press, New Jersey, 1976.

[32] Zhou, M.; Liu, X. B.; Yang, J. B. Evidential Reasoning-Based Nonlinear Programming Model for MCDA Under Fuzzy Weights and Utilities. // International Journal of Inteligent Systems. 25(2010), pp. 31-58.

[33] Zhang, Z. J.; Yang, J. B.; Xu, D. L. A hierarchical analysis model for multiobjective decision making. // Analysis, Design and Evaluation of Man–Machine Systems / Pergamon, Oxford, U.K. 1990, pp. 13–18.

[34] Jagnjic, Z.; Slavek, N.; Blazevic, D. Condition Based Maintenance of Power Distribution System. // EUROSIM / Attiya, G.; Hamam, Y. 2004, pp. 13-14.

[35] Xu, D. L.; Yang, J. B. Intelligent decision system for self-assessment. // J Multi-Crit Decis Anal. 12(2003), pp. 43–60.

Authors' addresses

Krešimir Šolić, dipl. ing.
J. J. Strossmayer University of Osijek,
Faculty of Medicine
Department of Biophysics Medical Statistics and Medical Informatics
Josipa Huttlera 4, HR-31000 Osijek, Croatia
kresimir.solic@mefos.hr

Prof. dr. sc. Franjo Jović, dipl. ing.
J. J. Strossmayer University of Osijek,
Faculty of Electrical Engineering
Department of Computer Science
Kneza Trpimira b.b., HR-31000 Osijek, Croatia
franjo.jovic@etfos.hr

Mr. sc. Damir Blažević, dipl. ing.
J. J. Strossmayer University of Osijek
Faculty of Electrical Engineering
Department of Computer Science
Kneza Trpimira b.b., HR-31000 Osijek, Croatia
damir.blazevic@etfos.hr