TECHNOLOGICAL AND ECONOMIC DEVELOPMENT OF ECONOMY
ISSN 2029-4913 print/ISSN 2029-4921 online

2013 Volume 19(4): 675–686
doi:10.3846/20294913.2013.861369

RAISING EFFECTIVENESS OF ACCESS CONTROL SYSTEMS BY APPLYING MULTI-CRITERIA DECISION ANALYSIS: PART 1 – PROBLEM DEFINITION

Leonardas MAROZAS, Nikolaj GORANIN, Antanas CENYS, Lukas RADVILAVICIUS, Zenonas TURSKIS

Vilnius Gediminas Technical University, Saulėtekio al. 11, 10223 Vilnius, Lithuania

Received 31 December 2012; accepted 29 October 2013

Abstract. Currently, control of access to information and physical resources has become extremely important. Numerous methods and solutions for architecture of systems aimed at controlling physical access are available; however, there is little information about application of Multi-Criteria Decision Analysis methods when evaluating separate logical components, needed for the design of access control systems and their interconnection in the final architecture.This paper is the first part of a two-part article, discussing application of multi-criteria decision making for architecture of access control systems. The first part defines the problem and discusses the possibility to use Multi Criteria Decision Making techniques when designing access control systems, including risk analysis for specific criteria and practical application of the developed model. In the second part, the possible solution model will be presented.

Keywords: multi-criteria decision analysis, optimisation, architecture of access control systems, risk analysis.

Reference to this paper should be made as follows: Marozas, L.; Goranin, N.; Cenys, A.; Radvilavicius, L.; Turskis, Z. 2013. Raising effectiveness of access control systems by applying multi-criteria decision analysis: part 1 – problem definition, *Technological and Economic Development of Economy* 19(4): 675–686.

JEL Classification: D81.

Introduction

Rapid growth of networking technologies has increased risks of information security. As the platform of interacting technologies becomes more advanced, the composition and characteristics of infrastructure and data accessing are becoming more dynamic and more

Corresponding author Leonardas Marozas
E-mail: *leonardas.marozas@vgtu.lt*

Routledge
Taylor & Francis Group

unpredictable (Jung, Joshi 2012). Access control systems (ACS) have different descriptions in the literature, but the main principle that remains the same – access control is the selective restriction of access to a place or other resource (RFC 4949 2007). They can be constructed in a variety of manners and based on physical attributes, sets of rules, lists of individuals or systems, or factors that are more complex. Recent developments of information technologies were very dynamic. Characteristics are (Tao, Zhang 2012) as follow:

- The number of transacting entities is not fixed;
- The relationship between these entities is very dynamic;
- It is possible that the transaction is conducted in a fully automatic approach.

Access control (AC) is one of critical security issues facing multi-agent systems. ACS aims at risk control, allowing or denying, limiting and revoking access. ACS can range from simple locks that keep outsiders away from private property to complex integrated security systems that combine different security methods – biometric systems, pin codes, radio frequency identification (RFID) cards, etc. Modelling of security policies, along with their realisation, must be an integral part of the network development process, to achieve an acceptable level of security for specific resources (Pavlich-Mariscal *et al.* 2010). Physical security takes a wider aspect. It also prevents unauthorised access to equipment, installations, material and documents, also protects against espionage, sabotage, damage or theft (FM 3-19.30 2001).

Decision support systems (DSS) are used to solve problems in different areas (Romano, Stafford 2011; Ghandforousha, Sen 2010; Moreira Barradas *et al.* 2012; Zhou *et al.* 2012; Dulčić *et al.* 2012; Urbanavičienė *et al.* 2009).

Effectiveness of ACS depends on multiple criteria. Nwamadi *et al.* (2012) proposed a multi-criteria ranking greedy algorithm for physical resource block allocation in multi-carrier wireless communications systems. Each of the criteria has different measurement units, different importance factors and depends on user rights and accessed object. Decision-making requires taking various points of view when dealing even with simplest objectives in design of ACS – finance, convenience, ethics, security, human resources, human rights, quality of service and more, depending on stake-holders or different requirements of the client. Development of ACS is a multi-criteria decision analysis (MCDA) problem. Ability of MCDA to solve problems of high uncertainty and deficiency of certain data is very important. One of the most important aspects of MCDA to be used in development of access control systems – it can deal with mixed sets of data, both quantitative and qualitative, including expert opinions. There are only few attempts (Azhar *et al.* 2012) to use MCDA when choosing a suitable access control system. There has been no methodology yet proposed for MCDA use in architecture of access control systems.

With increasing exposure and vulnerability to cyber-attacks and attacks related to security, it has become necessary to develop methodologies and systems that are capable of dealing with complex and multifaceted nature of decision situations encountered in security planning and management. For this reason El-Gayar and Fritz (2010) developed theoretical model of DSS, which is based on MCDA framework.

1. Basic model of an access control system

The first generation of electronic security systems dates back as far as to the middle of the 19th century when McCulloh loop alarm system was designed. The first generation of ACS is still widely used (Trimmer 1999). ACS from this generation are mostly standalone card readers. The second generation of ACS with centralised card readers and little use of CCTV emerged at the end of World War II and is still used today. The fourth generation (the third since one is obsolete and not used anymore) is important in terms of technical advances of separate AC units, their integration and merging. The basic scheme of the fourth generation model for access control systems is presented in Fig. 1.

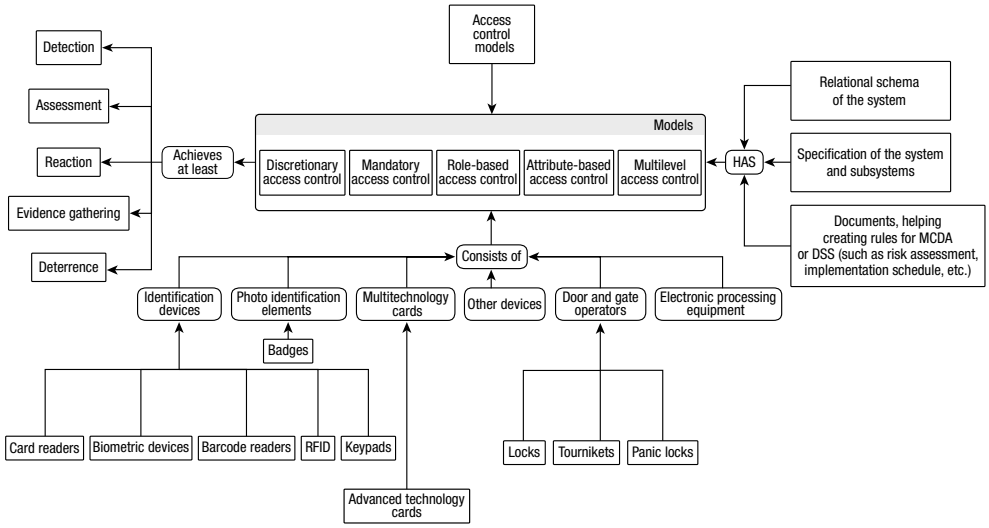

Fig. 1. Basic model of the fourth generation ACS

The main objectives and their priorities that are the basis for MCDA must be determined taking into account possible countermeasures, policies and procedures, budget and other factors.

There are three self-explanatory categories of countermeasures (Norman 2007):

- High tech countermeasures – electronic security systems, IT systems, phone security systems;
- Low tech countermeasures – locks, landscape, lighting, etc.;
- No tech countermeasures – policies and procedures regarding specific activities, security awareness, training, etc.

There are different methodologies that are used to determine countermeasures, but the main points that are outlined in them are as follow:

- Determination of critically sensitive areas with consequences and their weight (importance) values such as life loss, monetary loss, injuries, loss of business continuity, etc.;

- Threat analysis, including possible threat actors and attack vectors with their weight values – such as small thieves, terrorists, activists, anarchists or other actors;
- Evaluation of natural and existing countermeasures that do not need new implementations, but perhaps improvements – such as redistribution of lighting spots, etc.;
- Determination of likelihood of attack and risks;
- Determination of additional needed countermeasures and their prioritisation.

2. Model for determination of strategies and threats for an access control system

There are many available strategies to ensure AC. Indeterminate methods, such as brainstorming, lateral thinking (advised in De Bono 1977) and variation of inputs (people from different backgrounds offering their ideas), dominate among the methods for listing strategies and creating criteria trees. The aim of this research is to develop the use of attack trees in order to define threats for property and optimise the set of criteria for analysis as well as choose the best security strategies by using risk-based approach. The model consists of two main parts: (1) risk-based approach for selection of strategies and (2) multi-criteria assessment and determination of the most suitable strategies.

2.1. Risk based approach for selection of strategies

Risk-based approach is suitable for characterising specific values of an access control system in MCDA because of three strategies of risk-based approaches that can be closely associated with MCDA approach, as it is stated in (Klinke, Renn 2002):

- Risk-based approaches include numerical thresholds (quantitative safety goals, exposure limits, standards, etc.);
- Reduction activities derive from the application of the precautionary principle (examples are ALARA, i.e. as low as reasonably achievable, BACT, i.e. best available control technology, containment in time and space, or constant monitoring of potential side effects);
- Standards derived from discursive processes such as roundtables, deliberative rule making, mediation, or citizen panels.

Vandenbrink's flowchart of risk management standard ISO 27005 is shown in Fig. 2.

The numerical values that risk analysis presents could be used to find the solution to the MCDA problem.

This method is superior to very loose methodologies such as brainstorming and other, mentioned in the beginning of the chapter, since it has strict rules and step-by-step guide of how and what should be achieved during each step. The chart of the steps is shown in Fig. 3. During the process of risk analysis, tolerable level of risk is determined. This variable is later used to solve the MCDA problem.

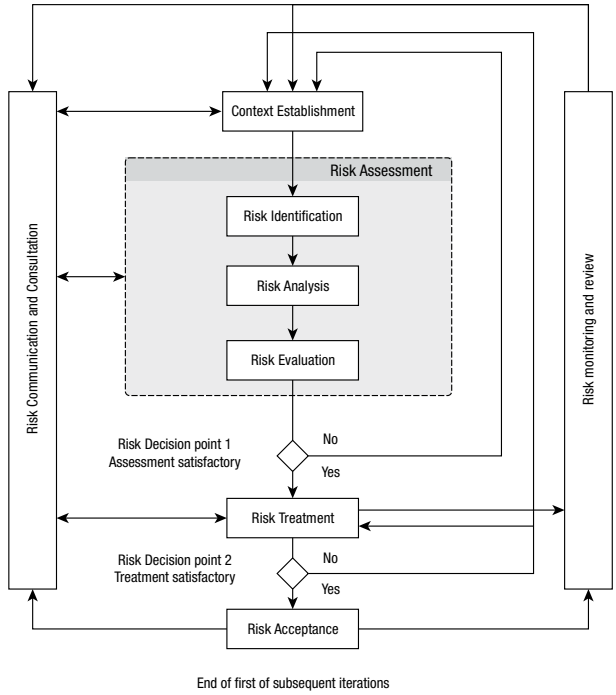

Fig. 2. Risk management standard ISO 27005 (Vandenbrink 2012)

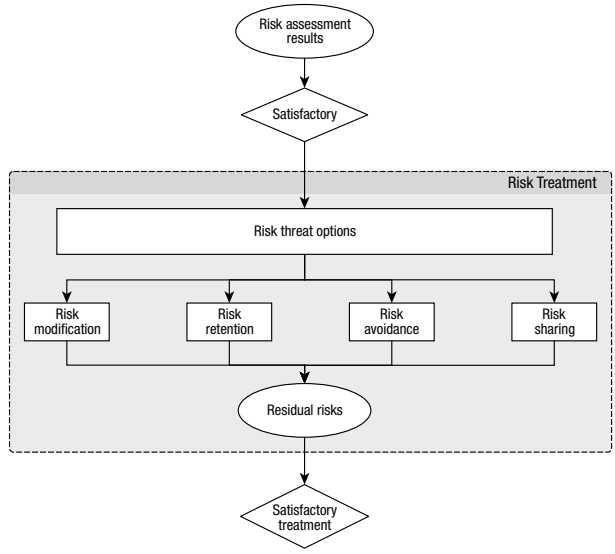

Fig. 3. Steps of risk assessment (Vandenbrink 2012)

2.2. Determination of threats using attack trees

General attack trees are constructed and presented in Fig. 4 (Ingoldsby 2009), having in mind the attacker, i.e. from the attacker's point of view. The top-level node represents the root node with the objective that in case of access, control systems will be getting inside the area or facility by using any of the vulnerabilities. The attack-tree approach allows finding all possible attack methods and their implementation scenarios.

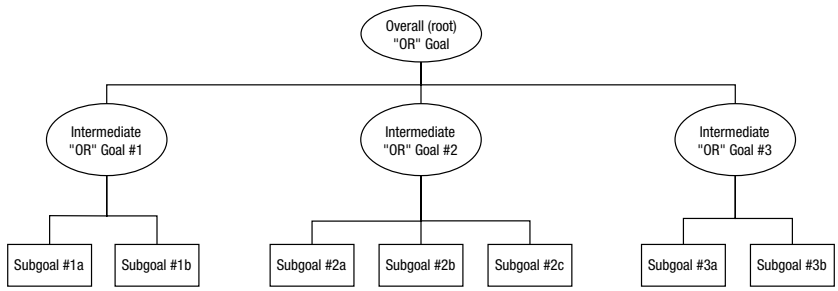

Fig. 4. General flowchart diagram of attack trees (Ingoldsby 2009)

Possibilities to enter an area or facility are very wide and when using non-formal approach, crucial values can be missed resulting in selection of an incorrect strategy and criterion.

Risk is usually calculated by combining two factors – attack probability and impact. This is important since in order to understand the risk and correctly evaluate the weights on criteria and strategies, model needs to include the impact that each of the attack scenarios could have on the victim.

3. Introduction of MCDA methodology for assessing control strategies

Developed model and determined steps of the methodology for ACS design are presented in Fig. 5. Two steps that need further explanation are listed below. First, the process should focus on the crucially important task: to determine the decision-maker and differentiate one from the problem analysis.

Different points of view are available for optimisation of the criteria tree and synthesising criteria into one optimality criterion (e.g. using cost benefit analysis in the fifth chapter of Getzner *et al.* 2004). The criteria tree is highly dependent on the priorities and strategies determined during the first step. The criteria set for assessment of ACS was determined based on risk analysis and investigation of attack tree peculiarities. It is presented in Fig. 6. The first step in building a criteria tree is deciding on the top-level criteria for ACS that will be broken down to smaller pieces during the process. These criteria could be cost, quality of service, speed of access, convenience and others. They exist in most other methods of MCDA, including general ones. Each group of criteria has different impact on decision weight (importance). The sub-criteria of each group have specific weights. Additionally,

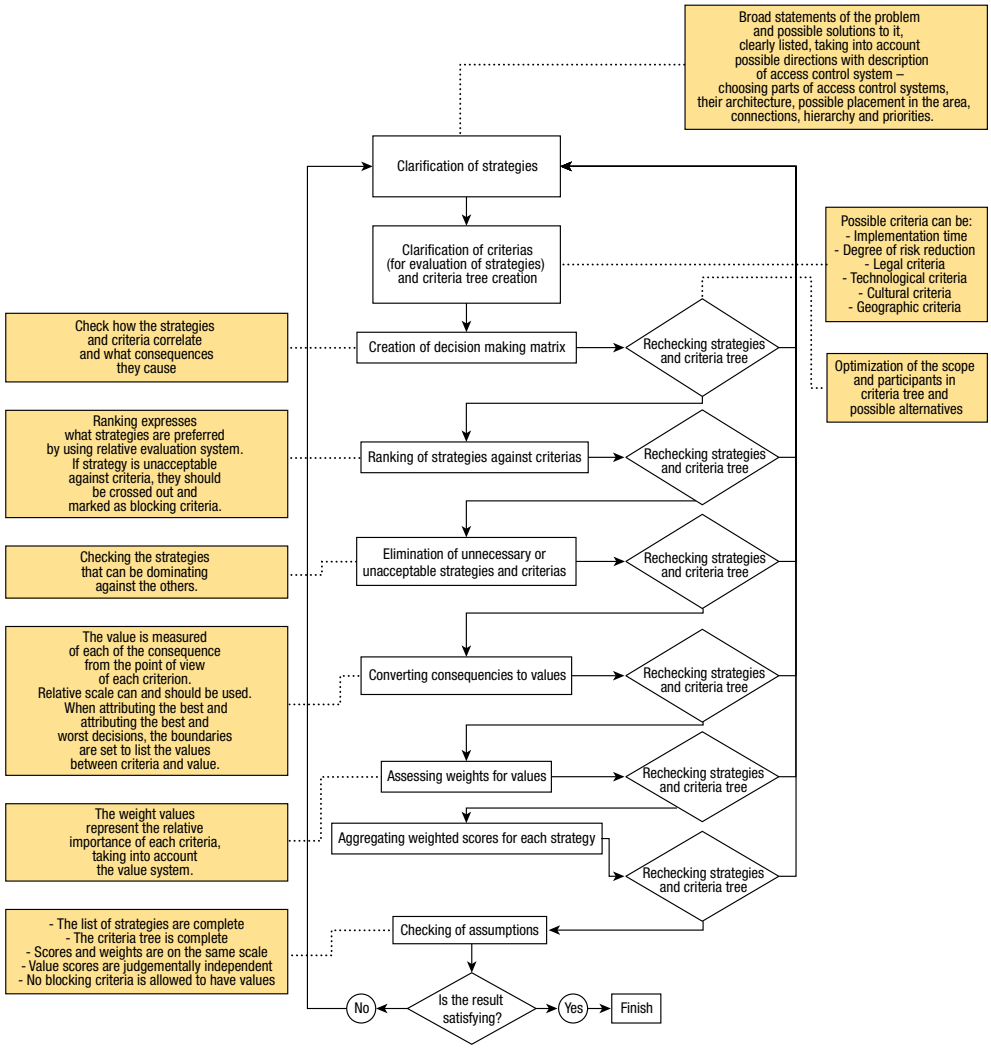

Fig. 5. Steps of MCDA for access control systems

there were six criteria established for ACS, in order to help designing the criteria tree while designing ACS:

- Implementation time. There might be additional security threats applicable to the public while the implementation of the system is not finalised;
- Degree of risk reduction. It is the most important criterion and it must always be less than the tolerable risk;
- Legal criteria. The use of technologies can be limited by legislation or directions of international units;

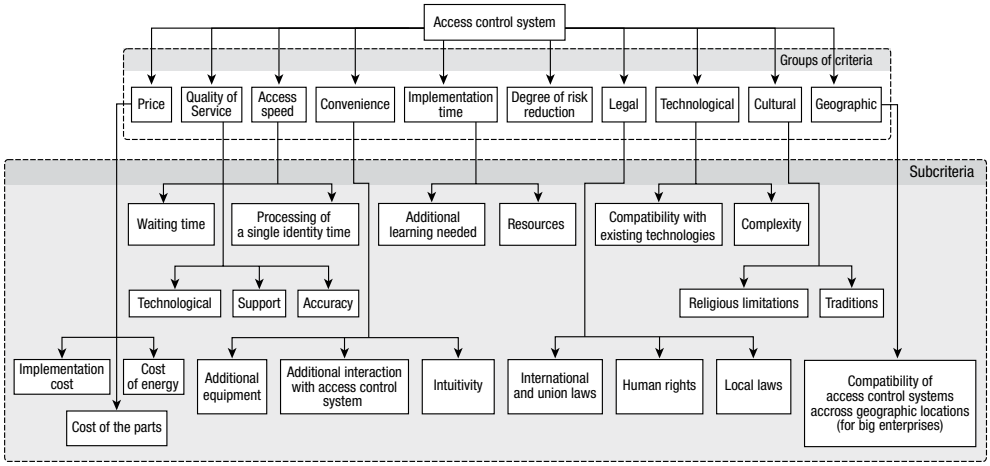

Fig. 6. Criteria tree for access control systems

- Technological criteria. There are not only advantages in using particular technologies, but also disadvantages – the more complex system and technology is used, the more difficult it will be to support and match the technology with existing ones;
- Cultural criteria are less strict than legal ones; nevertheless, they should be considered. For example, in countries of radical Islam, women cover their faces; consequently, the use of biometric ACS based on face recognition is pointless. In some cases, system users may feel treated as criminals (for example, in case of fingerprint based access control systems) and try boycotting the use of such systems;
- Geographic criteria are mostly used for bigger enterprises with offices dispersed throughout different geographic locations with different legal and cultural criteria, different technologies and technological freedom.

In terms of the tree, it is important to check for overlapping of criteria and ensure that all criteria are included in the tree.

When assessing weights for values for each access control application, the importance of each criterion is not necessarily equal for each user.

Therefore, for each criterion $c_j (j=\overline{1,m})$ a correspondiong weight $w_j (j=\overline{1,m})$ is assigned. $m \geq 1$ is a number of criteria under consideration.

The criteria weights for each user, transaction and problem under consideration could be customised as follows:

The customised criteria:

$$q_j = w_j \cdot k_j,$$

where q_j – customised criterion weight $(j=\overline{1,m})$;

$$m \geq 1$$

and k_j – customisation coefficient.

4. Reversing method and creating an access control system for optimised multi-criteria decision analysis values

In 2011–2013, while carrying out the project *Creation of manifold access control service system*, funded by MITA agency in order to create manifold access control system that would be universal and adaptable to otherwise diverse legal, cultural, technical and other requirements, analysis of access control systems according to the above developed model was made. Table 1 presents criteria using the designed manifold access control system.

In the current architecture, universal controllers can be used to connect with other controllers, readers, biometric controls or other sort of equipment in hierarchical or parallel way. Because of this sort of functionality, the size of the network of access points can be reduced or expanded on the go without additional grand architectural solutions.

Table 1. Criteria table for manifold access control system

Criteria	Remarks
Cost	Cost depends on client requirements. A network can consist of two controllers and few cheap RFID readers or key code panels.
Quality of service	It cannot be measured now, but the easy to use design and intuitive appearance should be easily accessible to the staff.
Access speed	Access speed is mostly determined by the end-point controllers. It depends on other factors identified by the client. If the client needs biometric access control system, it will be slower than RFID as well as more expensive.
Convenience	Convenience mostly depends on the end-point controllers that are used and previous experience of users.
Implementation	There are various ways to implement the whole network for access control system, but it is easy and intuitive.
Degree of risk reduction	Technically the degree of risk reduction is satisfactory for most of the small and medium enterprise.
Legal	It depends on the end-point controllers, but there are no legal issues with simplest RFID or key code locks in most of the countries.
Technological	Technological implementation and networking of controllers allow the client to avoid any technological issues.
Cultural	It is possible to avoid any cultural interferences by choosing the correct end-point controllers.
Geographic	Because of the universal character of the controllers of access control systems, they can be matched with almost any other equipment that operates according to widely accepted standards.

It is apparent that adaptation of multi-criteria decision analysis for the design of an access control system resulted in a highly flexible system based on multiple criteria. It can be adapted according to economic or technological needs of the client. In terms of the weighted value, the proposed system is superior to other systems that have been created using only technical evaluation.

Conclusions

The research developed a novel model, which is based on risk analysis and the possibility to apply MCDA of access control systems. The MCDA approach has an advantage versus commonly used purely technical analysis since it allows evaluation of not only technical parameters of access control systems, but also opposes them against economic, cultural, legal and other constraints, providing a balanced and economically reasonable decision.

The bigger part of the security externalities cannot be quantified in completely material manner since there are more components involved, such as prestige of the company, possible loss of clients or loss of service quality. Such factors are impossible to describe in a generalised model, but should also be included into a multi-criteria analysis. Similarly, it is impossible to correctly evaluate the effect of various normalisation methods or incorrect calculations while constructing a decision-making matrix and assigning values of weight.

It has been suggested to combine the multi-criteria evaluation of access control systems with generally used risk-based approach, common in implementation and development of information security measures. The main idea of the approach states that not only threat consequences should be evaluated, but weighted risks as well. Risk analysis should be applied not only while defining the strategy for an access control system, but also while evaluating different limiting criteria. Risk-based approach itself was integrated with attack tree method for identifying threats for access control system. Such integration provides a reliable method for identifying all possible threats and is much more convenient than commonly used brainstorming or checklist methods.

The criteria set for evaluating access control systems was determined. The application of MCDA methods allows making access control system more adaptable to rapidly changing environments. It makes an access control system more efficient in real time and uses extensive application domains.

This model is important in practical and scientific terms since it allows decision making in a complex process aimed at design of an access control system, taking into account different and often conflicting multiple criteria. Adaptation of the model was successfully used while designing a specific access control system.

Acknowledgments

The project *Creation of manifold access control service system* was financed under the high technology programme of MITA agency.

References

Azhar, A.; Amin, M.; Nauman, M.; Shah, S. U. 2012. Efficient selection of access control systems through multi-criteria analytical hierarchy process, in *Emerging Technologies (ICET)*, *International Conference Proceedings*, 8–9 October, 2012, Islamabad, 1–8.

De Bono, E. 1977. *Lateral thinking: a text book of creativity.* Harmondsworth: Penguin. 272 p.

Dulčić, Ž.; Višić, M. M.; Silić, I. 2012. Evaluating the intended use of decision support system by applying technology acceptance model in business organizations in Croatia, *Procedia Social and Behavioral Sciences* 58: 1565–1575. http://dx.doi.org/10.1016/j.sbspro.2012.09.1143

El-Gayar, O. F.; Fritz, B. D. 2010. A web-based multi-perspective decision support system for security planning, *Decision Support Systems* 50: 43–54. http://dx.doi.org/10.1016/J.dss.2010.07.001

FM 3-19.30. 2001. *Physical security.* Department of the army, USA 2010. 317 p.

Getzner, M.; Spash, C.; Stagl, S. 2004. *Alternatives for environmental valuation (Routledge explorations in environmental economics).* New York: Routledge. 306 p.

Ghandforousha, P.; Sen, T. K. 2010. A DSS to manage platelet production supply chain for regional blood centers, *Decision Support Systems* 50(1): 32–42. http://dx.doi.org/10.1016/j.dss.2010.06.005

Ingoldsby, T. R. 2009. *Attack tree-based threat risk analysis*. Calgary: Amenaza Technologies Limited. 32 p.

Jung, Y.; Joshi, J. B. D. 2012. Community based role interaction access control model, *Computers & Security* 31: 497–523. http://dx.doi.org/10.1016/j.cose.2012.02.002

Klinke, A.; Renn, O. 2002 A new approach to risk evaluation and management: risk-based, precaution-based, and discourse-based strategies, *Risk Analysis* 22(6): 1071–1094. http://dx.doi.org/10.1111/1539-6924.00274

Moreira Barradas, J. M.; Matula, S.; Dolezal, F. 2012. A decision support system-fertigation simulator (DSS-FS) for design and optimization of sprinkler and drip irrigation systems, *Computers and Electronics in Agriculture* 86: 111–119. http://dx.doi.org/10.1016/j.compag.2012.02.015

Norman, T. 2007. *Integrated security system design*. Elsevier. 472 p.

Nwamadi, O.; Zhu, X.; Nandi, A. K. 2012. Multi-criteria ranking based greedy algorithm for physical resource block allocation in multi-carrier wireless communication system, *Signal Processing* 92: 2706–2717. http://dx.doi.org/10.1016/j.sigpro.2012.04.020

Pavlich-Mariscal, J. B.; Demurjian, S. A.; Michel, L. D. 2010. A framework of composable access features: preserving separation of access control concerns from models to codes, *Computers & Security* 29: 350–379. http://dx.doi.org/10.1016/j.cosc.2009.11.005

RFC 4949: 2007. *Internet security glossary*. Version 2.

Romano, M. J.; Stafford, R. S. 2011. Electronic health records and clinical decision support systems, *Archives of Internal Medicine* 171(10): 897–903. http://dx.doi.org/10.1001/archinternmed.2010.527

Tao, W.; Zhang, G. 2012. Trusted interaction approach for dynamic service selection using multi-criteria decision making technique, *Knowledge Based Systems* 32: 116–122. http://doi:10.1016/j.knosys.2011.09.018

Trimmer, H. W. 1999. *Understanding and servicing alarm systems*. Butterworth-Heinemann. 272 p.

Urbanavičienė, V.; Kaklauskas, A.; Zavadskas, E. K.; Seniut, M. 2009. The web-based real estate multiple criteria negotiation decision support system: a new generation of decision support systems, *International Journal of Strategic Property Management* 13(3): 267–286. http://dx.doi.org/10.3846/1648-715X.2009.13.267-286

Vandenbrink, R. 2012. Cyber Security Awareness Month – Day 17 – A Standard for Risk Management – ISO 27005. *ISC Diary*.

Zhou, Q.; Yaoa, J.; Duan, W.; Liu, J. 2012. A knowledge-based decision support system for sulfur pricing, *Energy Procedia* 16: 784–789. http://dx.doi.org/10.1016/j.egypro.2012.01.126

Leonardas MAROZAS. He received Bachelor's and Master's degrees in Informatics Engineering from Fundamental Sciences Faculty at Vilnius Gediminas Technical University. He is employed at the Research Laboratory of Security of Information Technologies in Vilnius Gediminas Technical University. Currently, he is a PhD student in Informatics Engineering. His research results have appeared in journals such as *Electronics and Electrical Engineering, Journal of Vibroengineering, Geodesy and Cartography* and more. His research interests include biometrics and information systems security.

Nikolaj GORANIN. He received Bachelor's, Master's and PhD degrees in Informatics Engineering from Fundamental Sciences Faculty at Vilnius Gediminas Technical University. He is an Associate Professor at the Information Systems Department in Vilnius Gediminas Technical University. His research results have appeared in journals such as *Electronics and Electrical Engineering, International Journal of Computers, Communications & Control* (IJCCC), *Information Technology and Control* and more. His research interests include genetic algorithms, standardisation and IT security.

Antanas CENYS. He received his PhD in Vilnius University. He is the Dean of Science in Vilnius Gediminas Technical University. In 1999, he received the Lithuanian National Award of Science. He has more than 70 publications in journals such as *Electronics and Electrical Engineering, International Journal of Computers, Communications & Control* (IJCCC), *Information Technology and Control, Chaos, Solitons & Fractals* and more. His research interests include cryptography and network security, nonlinear dynamics in information technologies and electronic systems, nonlinear time series analysis in physics and biology, advanced mathematical methods and their applications, theory of chaotic systems and semiconductor theory.

Lukas RADVILAVICIUS. He received his Bachelor's, Master's and PhD degrees in Informatics Engineering from Fundament Sciences Faculty at Vilnius Gediminas Technical University. He is the CEO of "nSoft" company and works for the Research Laboratory of Security of Information Technologies in Vilnius Gediminas Technical University. His research work has been publicised in journals such as *Information Technology and Control, Journal of Engineering Science and Technology Review* and more. His research interests include antivirus technologies, access control systems.

Zenonas TURSKIS. He received his PhD in VISI (Vilnius Engineering Construction Institute, former name of Vilnius Gediminas Technical University). He works in Construction Department at Vilnius Gediminas Technical University. He has more than 100 publications in journals such as *International Journal of Information Technology & Decision Making, Economic Research, Journal of Economic Computation and Economic Cybernetics Studies and Research* (ECECSR) and more. His research interests include automated programming, technological decision multicriteria evaluation in construction and investment areas.