Factors of risks influencing the safety of the company and its strategy

J. Štofa, I. Zolotová

***Abstract*—** The paper focuses on corporate strategy for managing enterprise security. In paper is developed the issue of enterprise security policy and with that associated security project. The paper looks at the interaction of the company with a social web. With the implementation of security measure into company is developed also the topic of evaluation and quantification of risk. The paper points out the use of strategy of risk management as well as the importance of using modeling tools and itself business process modeling. They affect the security of enterprise, data protection and all assets which the company uses.

***Keywords*—** enterprise, process modeling, security, security project, social web.

I. Introduction

Information, which can today be obtained also through social networks, indicates the value of the company. It is therefore in place to continuously improve the safety rules and resources respectively methods used to ensure the safety. The company's assets must be protected and is important to treat them with responsibly. Such protection of personal data, sensitive and classified information solves also legislation, which directly provides binding rules and regulations concerning the protection of persons, property and information. Subject of safety of information in different companies is all information which is under to protection the relevant statutory provisions, e.g.:

- In EU:
  - o European Parliament and Council Directive 95/46/EC from 24 October about the protection of personal data and the free movement of such data [25]
  - o Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data
- In Slovakia:
  - o no.428/2002 Collection of Laws: Law on Personal Data Protection [3]
  - o Safety standards: MF/013261/2008-132, Standard ISO / IEC 17799:2005 [3]
  - o Methodical instruction, the Ministry of Finance of the Slovak Republic, no. MF/012943/2012-165, to evaluation of safety standards [13]

With regard to safety in the plane of businesses, it is necessary to point out that even in security is necessary to establish an effective control mechanism. Such a system should operate on the basis of pre-defined strategy, which is characterized by "instructions" - Plan, Do, Study and Act. Model of the control strategy is shown in Figure 1.

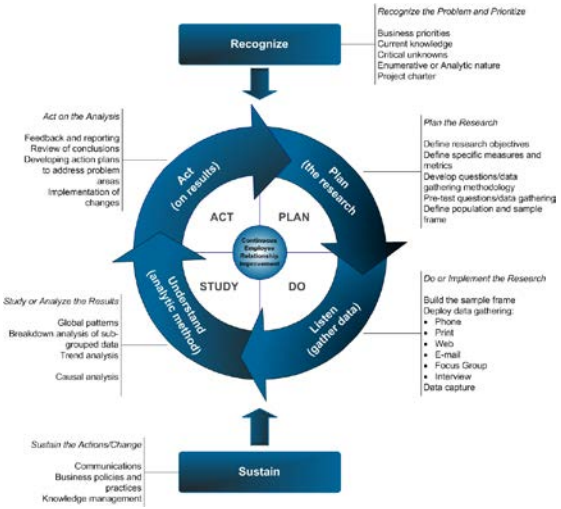

Figure 1 Deming´s model of control, source: [5]

Part of such safety management system is a security policy that carries in itself basic information about what and how the company tries to protect, and where is the center of his vulnerability. According to the abovementioned legislative documents is currently security project a feature of project management of company, which cover the mentioned issues. An important step for active security policy in an enterprise is to determine development of the security project, which is seen as a legal obligation [3].

Security project includes and emphasizes personal data of the persons concerned, while offers the possibility of effective protection of all company assets (data, metadata, physical and software sub-actives, human resources). Operators of businesses can through the security project to minimize or eliminate possible risks to all assets with which business operates. This security is not just puzzles of various orders and internal guidelines fragmented by individual departments. The emphasis is on security policy. Therefore, enterprise security project represents a clear and flexible document reflecting all aspects of the operation of the business entity and its protection. It has the role of internal "law".

The management of the enterprise must maintain the security continuously and effectively using all resources, which can ensure stable functioning of the enterprise at present, and the steady development in the future [1]. It requires an active approach of executives to be able to:

- identify immediate threat,
- identify possible ways of threats to security,
- identify the causes of potential threats to security,
- create such security system, which can effectively eliminate or minimize all potential risk of security incidents of all assets of the enterprise.

However, 21 century brings unprecedented opportunities for businesses to expand, enhance and promote their business. One such option is the promotion of business promotion through social networks [20].

Small and medium enterprises start to think more and more about establishing a corporate profile on social networks. It is a new level of communication with clients. This new phenomenon which interferes to business processes cannot be exempted from strict control. It must be integrated into an overall strategy for managing enterprise security.

II. Enterprise and its Relationship with the Virtual World

To look at the relationship between business and social web can be in many respects [12]:

- issue of monitoring employees' activities on social networks,
- corporate marketing,
- personnel management - selection of potential employees.

Mentioned aspects can be developed into processes. There are various methods and modeling tools. Created processes can take into account the different activities of employees and direct business activities in relation to them. Created process models help streamline business management strategy [24]. Also they contribute to the support of its security forces [16].

Figure 2 is a scheme of the most common uses of social web in the business environment.

Figure 2 The use of social web in business environment, source: [6]

III. Analysis of Factors of Risks

Analyses itself are mostly realized by templates for this purpose, in order to achieve unbiased results. Analysis of risk factors can also be classified according to the method of analysis. Basic division of analysis of risk factors [26]:

A. Model approaches - basic risk analysis model:

1. preparation of model - determine the mathematical relationship
2. identification of risk factors
3. determine the movement of factors of risk values at specified intervals
4. determine the interval of the probability distribution for each risk factor
5. determine the correlation relations
6. simulation - creating random scenarios based on a set of assumptions
7. analysis of simulation results

B. Identification of risk factors:

- Definition of risk:
  - based on knowledge, experience and intuition of managers
- Prioritization of risks:
  - probability of occurrence
  - intensity of the negative impact

C. Expert evaluation of risk factors:

Such evaluation is applied if they have risk factors bivalent nature of the random variables, that is, we assume that there may be only two situations - there is / there is no occurrence of a risk factor. Every manager should know not only the risk and its root cause, but also the characteristics of a possible adverse event. Risk assessment is the process of determining of its size by assessing the possible extent of the damage and losses that may result in a state of crisis.

Definition of the risk assessment consists of the following steps:

- short description of crisis situations
- definition of the period considered
- definition of the degree of probability
- determine the effects
- evaluation of all outbreaks of crises (assessment shall be entered into the form and transmits it to the matrix, the overall view of the crisis can then be derived strategy).

Expert evaluation is an essential tool for determination the significance of risk factors and overall risk determination. The significance risk factors are assessed using two ways:

1. probability of occurrence of the risk factor (can be expressed verbally or numerically, so-called subjective probability expressing beliefs of expert, respectively crisis manager on the possibilities of occurrence of risk events)
2. intensity of the negative impact of considered risk factor (assessment of risk factors can be realized by the method of scoring data obtained through brainstorming, Delphi method or brainwriting, where

it is found intensity of impact of risk factors on selected indicators of the entity). In addition to the quantitative assessment of the significance risk factors can also be useful certain graphical display. The data obtained are recorded in a matrix called. Risikomatrix. The result of the evaluation will be carried out by the expert list of the most important factors - the order of 10.

Tab. 1 Example of expert evaluation of risk factors

Factor of risk	Probability of occurrence	Intensity of the effect	Evaluation
FR 1	1	4	4
FR 2	4	4	16
FR 3	2	3	6
FR 4	3	2	6

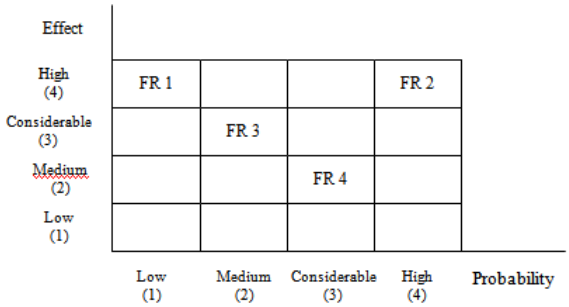

Figure 3 Example of expert evaluation of risk factors

D. Analysis of the sensitivity:

Sensitivity analysis is an important tool for determining the significance of risk factors and overall risk determination. Contrary to expert evaluations is based on explicit views the impact of risk factors of the entity and degree of its security. It can be expressed by different indicators that characterize the assessment process of systems.

IV. System Function of Factors of Risks

All human activities constitute individual and social positives as well as undesirable effects. In general they are called threats, risks. It is important to perceive the distinction between threat and risk. At present is a big problem with their definition. Experts define risk as a complex function of threats associated with specific social, technological or environmental system.

Mathematical definition of risk is very simple. Risk (R) is the product of the probability (P) (frequency) of an adverse event and its consequences (C):

$$R = P \times C \quad (1)$$

From this definition, it is evident that the risk is a quantitative term. This term includes probability of unacceptable (unacceptable) consequences of well-defined adverse events. Risk (R) is also the proportion of danger (threat) (D) and preventive measures (protection) PM:

$$R = T / PM \quad (2)$$

Follows from the above that:

- risk can be reduced by implementing preventive measures or various forms of protection from real threats,
- risk cannot be zero,
- actual awareness of the risk reduces the risk [18]

Figure 4 shows the factors, which influence the risks and threats, the enterprise resists to.

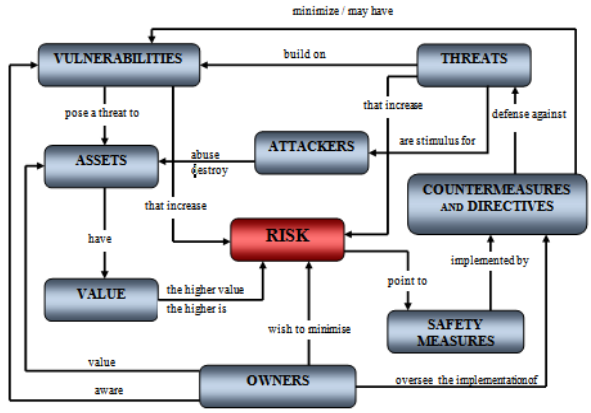

Figure 4 The system of risk factors, source: [4]

Enterprise tries all possible risks attacking its internal and external structure minimize to the line, when the potential risk may still be considered acceptable. This limit of acceptability is not fixed. Acceptable risk is classified as normal thing, which is safe, but it is possible to reach an improvement or to plan correction.

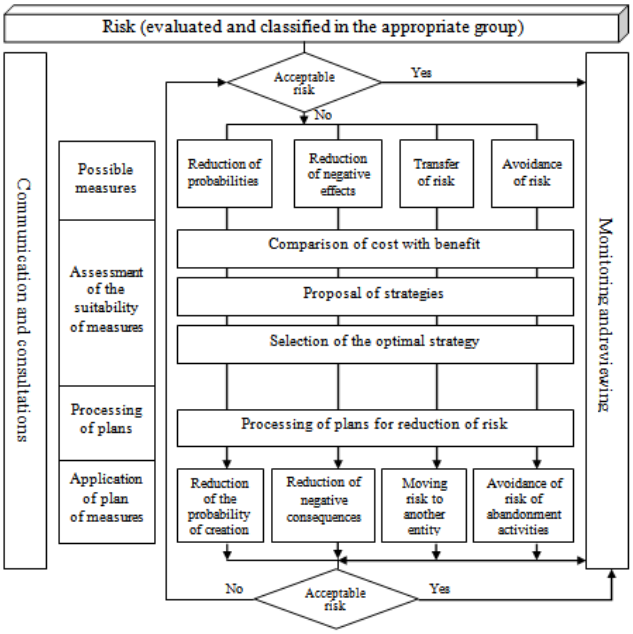

Figure 5 Process of minimizing of risk

Adoption of appropriate and relevant measures to minimize or eliminate threats the risk decreases. If adopted precautions are not sufficient, they should be reviewed and the company has to increase their efficiency [19].

The problem of definition and quantifying the effects of adverse events caused that we are not able to sufficiently credibly and especially objectively quantify the actual risk. Therefore are used different methodologies that are used to solve this problem. Existing methodologies in the evaluation of threats and risks can be divided into:

1. Induction methods ("ex ante") enable to predict the possible fault in the operating device file, and risk analysis points to factors that could cause failures. Help to evaluate the number and consequences of failures and take appropriate precautionary measures.
2. Deduction method ("ex post") analyzed resulting accident and looks for events and context that led to them [14].

Between well established and traditional methods belong [17]:

- Check List Analysis - CLA
- Routine Tests - RT
- Safety Audit - SA
- What if Analysis - WFA
- Rapid Ranking – RR

The original methodology for quantitative risk analysis of chemical processes CPQRA (Chemical Process Quantitative Risk Analysis) enriched the existing methods for identification of threats and evaluation of ensure of safety for new methods of risk analysis. It allows quantitative analysis of risk and to reconsider strategy of management of process security. CPQRA represents a tool for quantifying the risk and its minimization. It allows to identify and to determine priority of individual threats, which escalate degree of risk. For serious threats (sources of risk) may apply comprehensive measures to increase security. CPQRA methodology is also applicable for comparing different variants of process security solutions. Using a wide range of methods and procedures (which are part of the methodology CPQRA) allows elaboration of quantitative risk analysis. With them may be revealed significant sources of risk and on an objective basis can be recommended and designed necessary measures [18]. Comprehensive safety study, which analyzes risk with mentioned procedure, is ongoing study in sub-stages. In each stage is set up an intermediate target, e.g. threat identification. To resolve it may use any of the sub-methods. The recommended procedure includes the following sub-steps:

1. Determination of objective analysis by procedure CPQRA
2. Description of the analyzed system
3. Identification of threat
4. Establishment of the list of accidents
5. Selection of major accidents
6. Estimate of the consequences
7. Modification of the system in order to reduce the consequences
8. Estimate the frequency of occurrence of accidents
9. Modification of the system in order to reduce the frequency
10. Risk estimation based on the frequency and consequences
11. Modification of the system - reducing the risk.

V. Risk Management Strategies

Risk management is dealing with risks that may arise in the organization. It is a systematic process in which the risk identifies, analyzes and defines the optimal way to deal with it at minimal cost aspects and respect for the system entity's objectives. The task of risk management is primarily to maximize security and protect property by developing optimal management strategy as the main carriers of possible future damage [2]. The principal risk management strategies include:

- avoiding the risk
- risk-taking
- reduction of risk
- transfer of risk
- use of risk opportunities [23].

A. Reduction of risk

Process of risk reduction is very heterogeneous, which is clearly dependent on the nature of the specific risk, the probability of crisis phenomena, which can cause even from its anticipated negative consequences. Risk reduction is carried out:

- through the promotion of active anti-crisis policy:
  - appropriate structure for adopting security strategy and its implementation purposeful,
  - highlighting the positive development trends,
  - creating conditions that allow flexibility to respond to current threats,
  - permanent assessment of external and internal security conditions and taking into account in their decision-making processes,
  - efficient and economic organizational structure,
  - efficient personnel management and permanent training of workers,
  - respect for international and domestic legal standards and practices, but also moral principles,
- through the use of specific methods:
  - diversification of risk,
  - reduce the risk:
    - the underlying causes of risk
    - reduce the adverse impact of risk
  - retention of risk:
    - conscious and unconscious,
    - voluntary and involuntary,
  - risk sharing,
  - flexible procedure system
  - creation of reserves
  - permanent tuning of information (eg monitoring and warning systems)
  - avoiding risks,

- process optimization (using operational methods of analysis) [7].

VI. Modeling of Security of Enterprise Integrated in the Social Web

During our previous research [22] was shown that people neglect or ignore security and privacy of themselves. Users often share the most intimate details of their lives, which are available without any problem to anyone in the world. Moral and social boundaries between groups that are formed on social networks are disappearing. This rebus tries to decipher the low, which specifies the applicable rules and obligations for the protection of personal data available on-line [3].

Methods and tools for modeling business processes can be functionally used in the modeling of enterprise security as one of the most important strategy business management [10]. If the process of business management wants to be successful, the enterprise cannot forget to threats and direct attacks on its security. It is necessary to pay sufficient attention to the security aspect. Currently in companies is as a new „*helper*" social web, which entails a number of specific security solutions. One of the ways how can enterprises successfully prevent threats and risks arising from the contemporary phenomenon is to apply a process approach also to the level of security management.

With a suitably chosen modeling tool an enterprise can create models of business process including the possibility of employee work through a social network, identify the owners of the unique process and specify the persons responsible for their actions. An important part of security applications is assignment of clear and well-defined rules work and activity on the social web.

To apply the process approach to the issue of security management of enterprise we view from our perspective as a highly effective way of dealing with security - prevent threats and risks. In addition to the prevention of threats is on place to talk about detecting if you are in direct or mediated threats to the enterprise. Here we can count with process modeling solution, too.

Number of potential threats and risks can be predicted [8]. Although sometimes it is not possible to create a model whose implementation would automatically prevent any threat, there is still a chance to model the process of solving specifically problem, and therefore have a backup method of getting things resolved quickly and thereby avoid chaining attacks, or leakage of personal data and so on [11].

VII. Conclusion

The issue of business management strategy with regard to process modeling becomes crucial for addressing security by process modeling [21]. Integrated process modeling in business management can address a number of new problem areas arising from ICT progress.

It is known that it is easier to prevent problems than to face them. Business processes, as files describing progressively follow activities in the company, play a decisive role in the security balance. Attention turns to the processes in the company operating as a management tool of security. The modeling of these processes is an important factor in solving security problems. For implementing a process modeling is needed depth analysis of the automated and non-automated information system of company. Using it is possible to carefully identify critical points representing a threat to the company and its clients. It is analysis of risk assessment and measurement by an appropriate method chosen. Comprehensive and detailed models of business activities means an important step in the prevention possible attacks lurking outside, but also from inside of the company.

Enterprise which has in its plan flourish business through the social web and thanks that to be more visible should be protected in this way:

- understand what is important to be protect
- use strong passwords
- create a plan to be prepare for possible threats
- encrypt confidential information
- use reliable security solutions
- protect information completely
- ensure timeliness of security solutions
- educate employees.

Currently we work on the model of semi-automated process of evaluation the level of security of enterprise. It is a detection of vulnerabilities. The purpose of this tool is that on based of result of the evaluation to be able to show tools, measures and options to increase the current level of security of a particular company. This issue should be further developed by analysis of existing models of security evaluation and subsequent modification of the reference model of corporate security.

Creating a model of processing inputs and outputs analysis should ensure that they comply same comparison and evaluation criteria for all. Thanks that we will get a high comparability, credibility and objectivity of the results of analyzes. This reference model of security is considered part of the Security project created for a specific company. Creation of security project will also carry the intentions of capturing the behavior of company in communication with the virtual world.

Acknowledgment

This publication is supported by grant KEGA 021TUKE-4/2012 project (70 %) and grant VEGA 1/0286/11 (30 %).

References

[1] Application of Expert Method in the Process of Measurement and Performance Management / Adela Klepáková ... [et al.] – 2013. In: Recent Researches in Applied Economics and Management: Proceedings of the 5th WSEAS International Conference on Applied Economics, Business and Development (AEBD'13): 27.-29.August 2013, Chania, Crete Island, Greece. P.162-165. – ISBN 978-960-474-323-0 – ISSN 2227-460X

[2] Buganová, K. a kol.: 2012. Manažment rizika v podniku. 1. vyd. Žilina: Žilinská univerzita v Žiline. 2012. ISBN 978-80554-0459-2

[3] Collection of Laws n. 428/2002: Zákon o ochrane osobných údajov [cit 2013.7.21]. Available online: <www.zbierka.sk>
[4] Common Criteria for Information Technology Security Evaluation [cit 2013.9.21]. Available online: <http://www.commoncriteriaportal.org/files/ccfiles/ccpart1v2.3.pdf>
[5] Converge VoE Process Model [cit 2013.9.20]. Available online: <http://voiceoftheemployee.com/?page_id=11>
[6] Enterprise social technology: [cit 2013.9.21]. Available online: <http://www.enterprisesocial technology.com/blog/category/social-networking//>
[7] Hudáková, M. a kol.: 2013. Metódy a techniky v procese manažmentu rizika. 1. vyd. Žilina: Žilinská univerzita v Žiline. 2013. ISBN 978-80554-0642-8
[8] Identifying at-Risk Employees: A Behavioral Model for Predicting Potential Insider Threats: [cit 2013.9.10]. Available online: < http://www.pnl.gov/main/publications/external/technical_reports/PNNL-19665.pdf>
[9] Information Security [cit 2013.7.21]. Available online: <www.inoformacnabezpecnost.sk>
[10] Innovation processes - reference model, collaboration via innovative zone and integration into enterprise environment / Iveta Zolotová ... [et al.] - 2012. In: IFIP Advances in Infomatics and Communication Technology: Advances in Production Management Systems. Vol. 384(2012), p. 567-577. - ISSN 1868-4238
[11] Zolotova, I.: Measurement, classification and evaluation of the innovation process and the identification of indicators in relation to the performance assessment of company's innovation zones / Peter Kubičko, Lenka Landryová, Roman Mihaľ, Iveta Zolotová – 2013. In: Competitive Manufacturing for Innovative Products and Services: Advances in Production Management Systems, IFIP AICT, august 2013, Springer Verlag Series,ISSN: 1868-4238
[12] Landryova, L. Babiuch, M. Modeling Objects of Industrial Applications. In Handbook of Research on Social Dimensions of Semantic Technologies and Web Services. - Chapter XXXVI pp. 743-759, 1099 pages. Informatic Science Reference, Hershey, New York, IGI Global 2009. ISBN 978-1-60566-650-1
[13] Methodical instruction MF SR: MF/012943/2012-165, pre hodnotenie bezpečnostných štandardov [cit 2013.7.21]. Available online: <http://www.informatizacia .sk/index/open_file.php?ext_dok=14072>
[14] Methodological approach to the risk assessment of dangerous operations and study of companies in Slovakia: [cit 2013.9.10]. Available online: <http://www.sazp.sk/public/ index/open_file.php?file=cei/seveso/metodika_hodnotenie_rizik.rtf>
[15] Methodological approach to the risk assessment of dangerous operations and study of companies in Slovakia: [cit 2013.7.10]. Available online: <http://www.sazp.sk/public/ index/open_file.php?file=cei/seveso/metodika_hodnotenie_rizik.rtf>
[16] Perchè Facebook non è una Social Media Strategy [cit 2013.9.21]. Available online: <http://www.socialenterprise.it/index.php/2012/07/28/perche non-facebook--e-una-social-media-strategy>
[17] Process Management: [cit 2013.9.10]. Available online: <http://www.scss.sk/dvd_lpp_0384_09_2010/v%ddstupy%20z%20vlastnej%20vedecko-v%ddskumnej%20a%20pedago gickej%20%c8innosti/publika%c8n%c1%20%c8innos%8d/konferencie/sapria/mtfstu~3.pdf>
[18] Risk management: [cit 2013.9.10]. Available online: <http://fsi.uniza.sk/kkm/old/publikacie/ mn_rizik.pdf>
[19] Security revue [cit 2013.9.20]. Available online: <http://www.security revue.com/tbm/part1_a.html>
[20] Social media marketing industry report 2012 - how marketers are using SM to grow their businesses [cit 2013.9.10]. Available online: <http://www.socialmediaexaminer.com/SocialMediaMarketingIndustry Report2012.pdf>
[21] Štofa, J., a kol.: Process modeling as a supporting tool for managing of the enterprise security, In: IEEE 10th Jubilee International Symposium on Applied Machine Intelligence and Informatics, 26. - 28.1.2012, Herľany, Publisher: Óbuda University, Budapest, Hungary, 2012, 63-67, ISBN 978-1-4577-0195-5), IEEE Catalog Number: CFP1208E-CDR
[22] Štofa, J.: Bezpečnostný projekt podniku. Košice 2011, Technická univerzita, fakulta elektrotechniky a informatiky
[23] Strelcová, S.: 2012. Ekonomické teórie. Úvod do riadenia rizika. 1. vyd. Žilina: Žilinská univerzita v Žiline. 2012. ISBN 978-80-554-0541-4
[24] Supervisory control and data acquisition systems in virtual architecture buit via VMware vSphare platform / Miloš Pavlík ... [et al.] - 2012. In: Recent Researches in Circuits and Systems: Proceedings of the 16th WSEAS International Conference on Circuits (part of CSCC '12) : 14. - 17. July 2012, Kos Island, Greece. P. 389-393. - ISBN 978-1-61804-108-1 - ISSN 1790-5117
[25] The Office for Personal Data Protection [cit 2013.9.15]. Available online: <www.dataprotection.gov.sk>
[26] Varcholová, Tatiana - dubovická, Lenka. Nový manažment rizika. Bratislava: Iura Edition, 2008. 196 s. Ekonómia. VEGA 1/3809/06. ISBN 978-80-8078-191-0

Ing. Ján Štofa, PhD. student at Technical University in Košice, Faculty of Electrical Engineering and Informatics, Department of Cybernetics and Artificial Intelligence, email: jan.stofa@tuke.sk
J.Štofa was born in Košice, Slovakia. His scientific research is focused on data acquisition, process modeling, security project, social web.
Prof. Ing. Iveta Zolotová, CSc., professor at Technical University in Košice, Faculty of Electrical Engineering and Informatics, Department of Cybernetics and Artificial Intelligence, email: iveta.zolotova@tuke.sk
I. Zolotová was born in Michalovce, Slovakia. In 1983 she graduated (MSc) with distinction at the Department of Technical Cybernetics of the Faculty of Electrical Engineering at the Technical University of Košice. She defended her CSc. in the field of hierarchical representation of digital image in 1987. Since 2010 she's been working as a professor at the Department of Cybernetics and Artificial Intelligence at the Faculty of Electrical Engineering and Informatics at the Technical University of Košice. Her scientific research is focused on supervisory control, data acquisition, process modeling, human machine interface and web labs. She also investigates issues related to the digital image processing.