Human resources policy in relation to cybernetic security in Slovak medium and small companies

Benita Beláňová[1*]

[1]University of Economics in Bratislava, Bratislava, Slovak Republic

Abstract. Due to a mass penetration of information technologies into all business processes, researches in area of IS/IT field within medium and small companies has gained on significance. With the aim to acknowledge the status of information safety in the environment of Slovak medium and small companies a research has been carried out, which focused on identifying: threats on information systems; methods for treating information safety; and major obstacles in implementation of secure and safe policy. Within this research a special part was dedicated to companies' human resources policy in relation to cybernetic security. The research separately focused on staff provisioning in area of IS/IT. It surveyed who and on what position is responsible for this field, what requirements should be fulfilled by such people, which knowledge is the most valued and which they miss. The second area we focused on, was the organization of the security policy in relation to all employees, but mainly to users of information systems. The research was performed in the years 2008, 2012, 2015 and 2017 and the results about human resources are presented in this article. The respondents were company owners, managers and specialists form IS/IT field.

1 Introduction

Steering of medium and small companies has become a subject of economic investigation in the recent years. Regarding the influence of big organizations on national economy, the medium and small companies seemed to be not much attractive object of research and base for scientific knowledge implementation. The change in the mind-set was caused by new trends based on the acknowledgement of globalization and informatization in all areas of the private and corporate sphere [1-4].

Together with informatization there is a new field, which should be systematically managed and that is the security of information systems in the company [5]. The significance, which is attributed to the information security, is justified by an increased interest of companies about drafting, acknowledging and implementation of security policy. The information systems consist of information technologies, processes and people, and that's why human resource form an inseparable part of this policy [6,7].

* Corresponding author: benita.belanova@euba.sk

The employees of the company are the one, who represent one of the most significant threats in area of information security [8-11]. In generally, these employees can be split into two groups. The first group are the employees, who are responsible for administration and security of information systems and technologies in the company. In the second group there are the so called "passive users" of IS/IT, while mainly this group are the weakest element in the security of information in a company. Not only because of the fact, that the users generally don't read guidelines and so they don't follow any rules, but also because they like to experiment by breaking essential principles of security. These two groups of employees should be assessed separately within human resources policy in relation to information security of the company, as the expectations and requirements on their knowledge and skills diametrically differ. Furthermore, their place in the hierarchy of the company is diverse. While the first group can be easily identified a localized in the company's structure, the passive users of IS/IT range from managers to the lowest level of executive employees.

2 Results of the research

Presented results are partial outputs of a larger project mapping the development of information security in small and medium-sized companies in Slovakia. The first part of this research was passed out in 2006, followed by a much wider range in years 2008, 2012, 2015 and 2017. Respondents responded to 105 questions, divided into 15 thematic units. One area was also personal staffing.

The results of the research are presented in the following structure:

- Methodology and Research Methods
- Features of the investigated sample
- Results of investigation in area of human resources provisioning of IS/IT security
- Results of security policy investigation in relation to people – employees of the company

2.1 Methodology and Research Methods

The method of analysis, which allows for the breakdown of the whole into its individual parts and elements in order to know the sub-system as much as possible, has been used to analyse the current state of affairs regarding this issue at home and abroad, and we have combined the knowledge gained into a new whole by using the method of synthesis. Using the method of comparison the theoretical part was compared with opinions on the given issue and the terminological apparatus was subsequently specified by method of abstraction. The descriptive method is used to describe the principles of security information system management.

In the testing process, we investigated the hypotheses using one of the exploration methods - the questionnaire method. When applying this investigative method, the information obtained from the investigated subjects is gathered by querying, i.e., by deliberately targeted questions. This method makes it possible to obtain more information about the individual respondent at the same time. This information may relate to the extent and depth of the respondent's knowledge, preferences, past, present, or intended behaviour, and the characteristics of the respondent. Detection methods can be used to examine any phenomena, that is, companies of different sizes, different industry structures, ownership, etc. The application of detection methods can be adapted to both descriptive and causal research. For proper analysis and subsequent comparison of phenomena, it is essential that the analysed phenomena occur under the same conditions. Otherwise, erroneous

conclusions about the causes and consequences of the phenomenon due to the complexity of the conditions of economic life may occur.

Therefore, in order to obtain relevant and quantifiable information on the state of the security of information systems in small and medium-sized enterprises in Slovakia, the enterprises were sized according to the European Commission's directive no. 96/280 / EC, according to the industry classification of economic activities of SK NACE Rev. 2, then according to the legal form and ownership of the enterprise. The questionnaire was processed in electronic form. The MS Access database and the MS Excel spreadsheet were used for processing. Mathematical and statistical methods were used to evaluate the questionnaire. The results were transformed into tables and graphs.

By comparing the phenomena in time and space, we have identified, on the basis of the questionnaire survey, the common and different aspects of the behaviour of individual types of enterprises. The induction method allowed us to explore all available phenomena and their parts to generalize the results obtained.

2.2 Methodology and Research Methods

The research has been performed on a sample of randomly chosen medium and small companies in the Slovak Republic. A questionnaire was created in line with a template on the information security survey in the entrepreneur environment in Slovakia, which was carried out by the National Security Authority in cooperation with the magazine DSM – Data Security Management and company Ernst & Young in the years 2006 [12] and 2008 [13] and the Guideline on performing security audit of IS [14].

The research in the form of moment observation and random selection has in comparison with intentional interviewing of an earmarked group of companies selected in advance certain deficiencies. However, the objectivity of the results is justified by the high number of companies and their considerable sectorial variety. 247 companies took part in the research in the year 2008, 129 in 2012, 209 in 2015 and 219 companies in 2017. According to the legal form, the highest participation was represented by limited companies. According to the structure of the ownership, companies with exclusively local ownership or mainly local ownership prevailed.

2.3 Provisioning of human resources in area of information security

Qualitative provisioning of human resources is one of the basic and inevitable conditions for the execution of security policy of IS in the company, therefore it is necessary to give special emphasis on this factor [15]. More specifically on the definition, creation and staff occupation of roles, which ensure a continuous development of information security in the company that is in line with new legislative elements, organizational changes or evolution of the society, IS changes and finally in line with the security documentation itself [16].

Key roles, that in practice present the primary element of each steering system of information security should respect the existing elements of the company’s management (e.g. linear or process steering, expert competence etc.). The creation of these roles doesn’t necessarily require creation and occupation of new positions, as often a new role is allocated to existing employees. It is however important, that the respective roles ensure the execution of rules and principles specified in the security policy and their practical application and respect [17].

Within our research we have been investigating how is the field of information technologies included into the organizational structure and on which hierarchical level is

the information security. Nonetheless, the expectations, which are required from the employees involved in IS/IT and information security are significant.

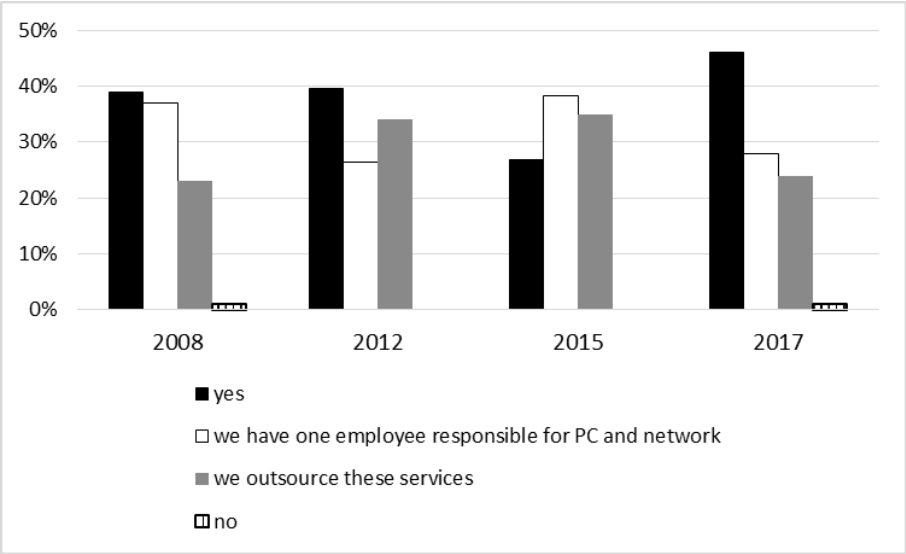

Fig. 1. Does your company have a separate business area responsible for PC services?
Source: own elaboration

Usually a business area specifically responsible for information technologies and systems in general is present in medium sized companies. In small companies this share is much lower. Small companies usually dispose with one person, who is in the position of network administrator and takes care about the operation of the information systems in the company. There are almost 10% of companies, mainly medium sized which dispose with employees, who are specifically involved into information security as their main work objective. The usual practice is to combine the information security with the IS/IT department. Companies, which don't have such department or administrator, get these services outsourced. In such cases, mostly in small companies, which get these services outsourced, no one is responsible for the security of IS itself (no department). Companies using the network administrator, usually pass the responsibility onto the economic and financial department.

The research has revealed the fact, that the information security is not integrated into business processes of the companies. In case of a separate solution regarding information security and risk management, an inadequate usage of company's resources just like a weak coverage of business risks, which come hand in hand with security risks on the level of information systems, may happen [12].

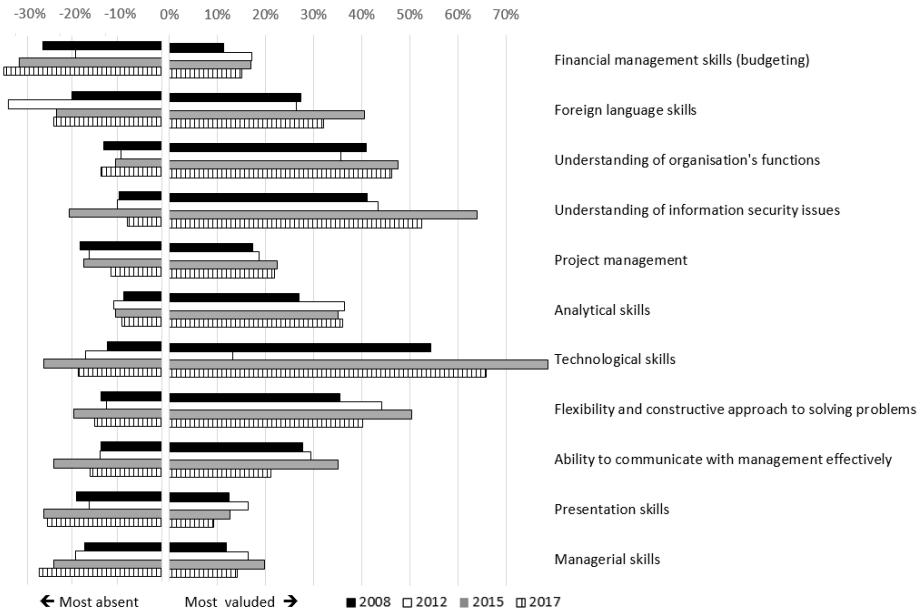

Fig. 2. The most absent and most valued knowledge and skills of information security staff
Source: own elaboration

We have found out a notable shortage of knowledge and skills of employees from the field of company's financial management, what we don't consider as a that much significant factor in the area of IS/IT, when comparing the most valued and on the contrary the most absent knowledge and skills of employees from the field of securing information systems. It is much worse in the field of technological skills of IS/IT and presentational and managerial skills, which belong to the key skills of IS/IT employees. The knowledge of foreign languages of the employees working in the field of information security has in comparison with previous periods improved, however still missing in 23% of companies. The respondents of the research considered technological knowledge of IS/IT, factual knowledge of the information security problem and flexibility and constructive approach in problem solving as the most valued knowledge and skills. The skill of an effective communication with the management of the company recorded a significant drop, when comparing to previous research. This is probably connected with the growing skills of employees in this field, hence their deficiency has proportionally decreased at the same time.

With regard the representation of IS/IT employees in the company, 1/4 of the companies considers the existing state as insufficient. A significant fluctuation of these employees was detected by 10% of companies. The compliance between the expertise and requirements is present at 2/3 of companies. The rest of 1/3 companies consider knowledge and skills as insufficient, or only partially compliant with the set requirements.

One of the reasons of this situation may be the financial compensation of these employees. The salaries of employees, who are responsible for IS/IT area in the company copies the development of salaries in Slovakia. In terms of time, there is an obvious shift from lower salary grades of employees responsible for information security into higher grades. However, we cannot claim that these salaries would reach a higher standard level, as it is in other matured economies, what leads to continuous deficiency of this qualified workforce, respectively to its fluctuation. Income over 2000€ were recorded in the segment of Business and Transportation.

Table 1. Gross average monthly remuneration of employees responsible for information security.

Salary	2008	2012	2015	2017
less than 500 €	42%	24%	16%	21%
501 – 1 000 €	37%	35%	34%	23%
1 001 – 1 500 €	11%	22%	31%	31%
1 501 – 2 000 €	6%	12%	14%	24%
more than 2000 €	4%	7%	5%	1%

Source: own elaboration

2.4 Security policy of the company in relation to other employees

Basic criteria were chosen to evaluate the security policy of the company in relation to "passive users". These criteria are considered from the IS/IT security perspective as main assumptions for security policy operation in medium and small companies. In the case of employees from the IS/IT field responsible for security, the fulfilment of these evaluation criteria is taken for granted.

The first evaluation criteria are trainings. The basic objective of the training in general is to increase the awareness of the employees about possible risks and instruct them, how to avoid these risks, or how to act in case a certain situation/state occurs. Regarding the security of IS/IT we can talk about rules on safe HW and SW usage, on safe data manipulation in the information system, their protection, policy of passwords and others. Employees should attend such trainings at least as newcomers. It is however desirable to organize such trainings periodically; the optimal frequency is one year. According to our research (2017) 39% of small and 56% of medium companies organize trainings on protection of data and usage of passwords.

In connection with the security policy, it is necessary to treat the leaving employees, where all access, manipulation and entering authorizations and means should be retained, or access passwords which the employee dispose with should be changed. As demonstrated on the Fig. 3, there is a percentage of companies, on average about 15% higher than in trainings, which follow this procedure.

The situation is worse in keeping written documentation about granted entering and access authorizations of employees to respective applications. When commenting these results, it should be stated, that in all monitored parameters in security area there is a decrease in 2012 in comparison with 2008. We link this phenomenon to the then ongoing economic crisis, when the companies had to cut their costs and the trend was to cut the costs mainly in security.

The access password is the main significance of the company's and its employees approach to information security. It is the simplest, cheapest and most effective security element which protects unauthorized penetration into the system. However, the practice shows, that companies don't focus sufficiently on password creation and definition of access rights within their security policy, as they should have. The rules of password creation are an internal matter of each company, just like the principles that should be followed when creating a strong, memorable password. These should be defined in the internal guideline of the company, with which should be all employees familiar (at least when joining the company). It is very usual that the employees have within applications the same access rights or that these rights are not specified in writing within their function. From this reason, we have specifically looked to the problemacy of password creation, their form and manipulation with them.

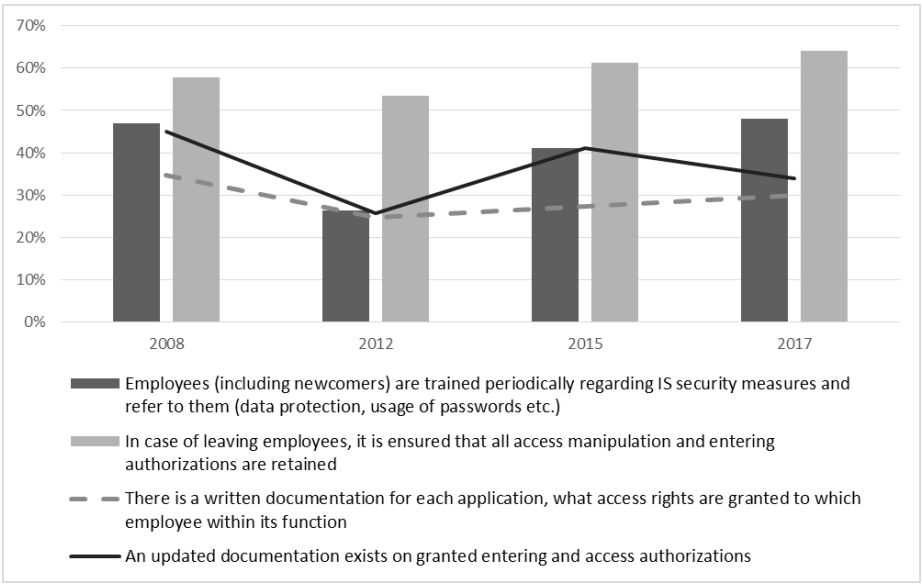

Fig. 3. Security trainings and documentation about access rights and data protection
Source: own elaboration

The outcome of the research presented, that more than 80% of users have an access password. However, the results confirmed that at least a half of them use the same access password to more applications, thus there is an increased risk from violation of more programs with the breach of one password. Furthermore, not all applications require to enter an access password. The main problem in password creation is, that they don't contain sufficient number of symbols and proper combination of symbols, which would prevent them from password breach.

Table 2. The number of symbols in the access passwords of employees

Number of symbols	2008	2012	2015	2017
More than 8 symbols	5%	6%	13%	30%
8 symbols	**22%**	**40%**	**42%**	**57%**
Less than 8 symbols	64%	54%	32%	14%

Source: own elaboration

In 2008 the most frequently used password was with the length of 5 and 6 symbols. In 2017 a more than a half of users have a password with 8 symbols, what is taken as a positive trend. The entrepreneur practice showed, that the security standard of an unbreakable password in all business applications is a predefined password format for server operation systems Windows from Microsoft, which requires a minimum of 8 symbols, 1 small letter, 1 capital letter and one digit. We haven't investigated on the password composition, but as we can see, already 30% of companies use a password with the length of more than 8 symbols. According to experts on information security, by adding 2 symbols you can substitute the missing capital letters, digits or random signs in the password.

A safe password is a password which change in regular interval. It is recommended that this interval takes 2 months. However, the entrepreneur practice showed that this safety rule is not kept in the companies. In 2/3 of the addressed companies, the passwords are not

changed during the overall operation of the systems and it is not usual to monitor and protocol any attempts of unauthorised access or breach of authorization.

Even the most perfect password is useless, when the employees don't use it in line with the purpose, for which it was created. Usually, the employees sign off and turn off their PC at the end of the working time, but they automatically don't, when they leave their working place, e.g. for lunch. In the years 2008-2015 we have encountered a group of employees, who didn't turn off their PC at all. This trend was however decreasing and in the year 2017 it didn't appear at all. Despite of this, there is still a big group of employees, who don't sign off their workstation during their absence, creating thus suitable conditions for data manipulation and undesired information outflow inside the company. According to our findings, 65% of companies recorded internal unauthorized access.

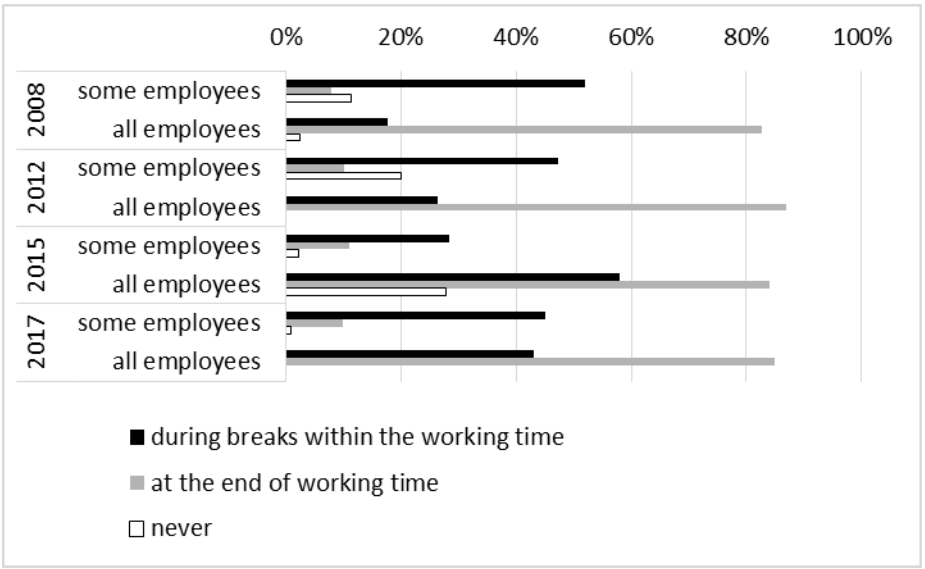

Fig. 4. Employees turning off/signing off PC
Source: own elaboration

3 Conclusion

The risks of the information security are caused by various threats, which influence vulnerable points of the company's information and communication systems. In the article we have focused on one of these – the human factor. Especially we were interested in investigating how the companies treat their cyber security in relation to their own employees. The conducted research brings more knowledge and outcomes for the area of information security management focusing on human resources. Resulting from the problem as it stands at present, we can confirm that 41% of companies create only a basic information security management structure, that is reflected also in the recruitment process of employees for this area and total costs incurred in connection with security awareness and employees acting safely. 13% of employees doesn't develop any kind of activity in this area.

If the companies want to reach an adequate level of their information assets security, they need to activate and effectively link all management processes, including management of human resources. In order that the company would fulfil the new requirements, it should change the basic awareness of its functioning. The organizational structure should be taken

as a basis, as a firmly defined distribution of activities, relations and competencies, resulting in present responsibilities and financial compensations.

With regards the employees in general, just like in other managerial disciplines, it is not easy to make a universal guidance on managing people and forming security awareness, that should be followed to achieve a guaranteed success. It is influenced by several factors, such as the size of the company, field of operation, structure of employees and other. According to our view, we have chosen the basic aspects and principles that should be followed by all types of companies. As can be seen from the results, the companies have significant deficiencies in effective application of security policy in relation to employees.

As we know, the research of information security in small and medium-sized companies in Slovakia has not been implemented to such an extent and such a focus by any other organization and we have no knowledges that a similar research was realized in any other country. Therefore, we can not compare our results with another similar research.

The gained results don't mean the termination of research activity in the field of information security management, but they provide further knowledge on the development of this problem and consequent assessment in the following periods.

The article was elaborated within the VEGA project no. 1/0309/18 Social Networks in Human Resources Management.

References

1. V. Bolek, A. Romanova, P. Richnak, K. Porubanova, The use of pervasive technologies in business processes. *Ad Alta-Journal Of Interdisciplinary Research,* **9**, 2, 293-298 (2019)
2. A. Romanova, P. Richnak, K. Porubanova, V. Bolek, Application of modern information technology in innovation of business logistics processes. *Ad Alta-Journal Of Interdisciplinary Research,* **9**, 1, 245-248 (2019)
3. M. Kokles, A. Romanova, A. Hamranova, Information Systems in the post-transition period in enterprises in Slovakia. *Journal of Global Information Technology Management*, **18**, 2, 110-126 (2015)
4. A. Hamranová, Š. Marsina, P. Molnár, F. Okruhlica, Development of Information and Communication Systems within the Building of Project-Oriented Manufacturing Organization. *Advances in production management systems: innovative and knowledge-based production management in a global-local world, pt 1 Book Series: IFIP Advances in Information and Communication Technology*, **438**, 241-+ (2014)
5. F. Korcek, V. Bolek, A. Romanova, P. Richnak, Practicing information security management system in e-commerce. *Ad Alta-Journal Of Interdisciplinary Research,* **8**, 1, 207-212 (2018)
6. D. G. Moody, M. Siponen, S. Pahnila, Toward a unified model of information security policy compliance. *MIS quarterly*, **42**, 1, 285-+ (2018)
7. Y. Zhang, Y. L. Zhang, J. Zhou, L. Liu, F. Chen, X. He, A review of compressive sensing in information security field. *IEEE access*, **4**, 2507-2519 (2016)
8. J. D'Arcy, P. B. Lowry, Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, **29**, 1, 43-69 (2019)
9. V. Bolek, A. Látečková, A. Romanová, F. KORČEK, Factors affecting information security focused on SME and agricultural enterprises. *Agris on-line Papers in Economics and Informatics*, **8**, 4, 37-50 (2016)

10. P. Balozian, D. Leidner, M. Warkentin, Managers' and employees' differing responses to security approaches. J*ournal of Computer Information Systems*, **59**, 3, 197-210 (2019)
11. P. Ifinedo, Roles of organizational climate, social bonds, and perceptions of security threats on IS security policy compliance intentions. *Information Resources Management Journal*, **31**, 1, 53-82 (2018)
12. PSIB SR ´06, Ernst & Young, NBÚ SR, DSM – data security management, TATE International Slovakia. http://www.dsm.tate.cz/cz/psib-sr-2006/ last accessed 2007/09/11
13. PSIB SR ´08, Ernst & Young, NBÚ SR, DSM – data security management, TATE International Slovakia. http://www.dsm.tate.cz/cz/psib-sr-2008/ last accessed 2009/05/06
14. Guideline on performing security audit of IS FM SR, 331/2003-22 (2003)
15. M. Szarková, M. Andrejčák, Personnel audit in financial institutions in Slovac Republic. *International scientific conference Financial management of Firms and Financial Institutions,* Part III, 899-902 (2013)
16. N. Matkovčíková, Health and safety management in companies of all size. *International scientific conference Hradec Economic Days 2017*, 597-603 (2017)
17. J. Koubek, *Řízení lidských zdrojů* (Management Press, Praha, 2015)