https://doi.org/10.15414/isd2018.s10.14

INFORMATION SECURITY IN AGRARIAN SECTOR OF THE SLOVAK REPUBLIC

Roderik virágh[1], klára hennyeyová[2], Edita šilerová[3], Galina Gerhátová[4]
Slovak University of Agriculture in Nitra, Slovak Republic[1,2,4]
Faculty of Economics and Management, Department of Informatics
Tr. A. Hlinku 2
Nitra, Slovakia
Czech University of Life Sciences Prague[3]
Faculty of Economics and Management, Department of Information Technologies
Kamýcká 129
Praha 6 – Suchdol, Czech Republic
e-mail[1,2,3,4]: roderik.viragh@uniag.sk, klara.hennyeyova@uniag.sk, silerova@pef.czu.cz galina.gerhatova@uniag.sk

Abstract

Every section of the national economy uses information and communication technologies for their activities, not excluding the agrarian sector. Although the agrarian sector in the Slovak Republic is less attractive for employment, there are still granges and small farmers who maintain the national tradition of agriculture. But for their better development and management they use modern information and communication technologies. These technologies can not only provide statistical information or keep records of increments, crops, etc. but also with their help work on fields is more efficient, e. g. with the help of drones. To keep these technologies in good condition the security of these technologies is important. This article is about information security, mostly the non-technical means, and oriented on granges of the Slovak Republic. The main focus is on information technologies, information systems and information assets used by these segments of the national economy. A questionnaire survey was conducted on granges of the Slovak Republic as a part of project KEGA (012SPU-4/2017) "Methodological manual processing Enterprise security policy" for mapping the current information security in this sector. The way of managing information and communication technologies is closely linked to the security of these technologies. There are some interesting differences between the management of ICT and their security – the way granges are interested in this topic. The risk analysis is directly connected with non-technical security means for *protecting ICT. These means are the Security Project and Security Policy documents. These documents contain the risk analysis to be performed in certain time intervals. The Security Policy contains every rule of protection of ICT and IS as other assets of a company. However, the Security Policy and the Security Project are the basic security means for assets of a company, only small number of companies and even granges develop, apply and adhere them.*

Key words: *Agrarian sector, Information and Communication Technologies, Information Security, Security Policy*

JEL Classification: *O34, O39*

1 Introduction

Information technologies and data which we process and use with the help of these technologies are inseparable part of the national economy and individuals. Even at work or in private we use information and communication technologies, e.g. personal computers, smart phones, smart TV, etc. In private we are responsible for the security of our ICT as at work. One cannot rely on other person or some technology to protect him from information threats on used information technologies. These threats may be of a technological or physical nature. Most threats are from the Internet because internet connection is almost everywhere by WIFI networks, mobile networks or cable connection. It is also important to oversee the physical security of these technologies. The agrarian sector in the Slovak Republic also uses information technologies more often not only for data processing, but also for direct help at daily work, e.g. GPS when working in the fields, drones for land mapping, automatic feeders, etc. For this reason, these technologies must be protected also in this part of national economy. The article focuses in survey on the state of the information security.

Usage of information and communication technologies has a direct impact on the development and competitiveness of individuals, firms, production sectors, regions and even the whole continents. It is possible to state that the general characteristics and principles of ICT usage in the agriculture sector are beyond and doubt valid and will be valid in the future (Jarolímek and Vaněk, 2003).

Similar research was conducted on agrarian cooperatives by Montegut-Salla, Y., Cristóbal-Fransi, E., and Gómez-Adillón, M.J. (2013). They focused mostly on used information and communication technologies and Internet in agro-food cooperatives. The research addressed the following aspects: computer equipment, Internet connection and presence and the level of electronic commerce.

IS/ ICT assets include the technologies, applications, data and also people. Examples of the assets are hardware, software tools, data that the field of informatics uses and processes. It also includes the standardized and formalized processes and knowledge included in the informatics, as well as individuals – operational staff, managers of individual applications (Gála et al., 2006)

Development of information and communication technology also led to development in data visualization methods. There are many tools for monitoring of moving objects in agrarian sector, and also many different approaches on how to access and utilize location data. The suitability of given solution depends mostly on user requirements. Every user group has different demands and rights when operating software tools, especially GIS (geographic information system). (Pavlík, J., et al., 2015) These methods are not described in the paper, but there are important for the knowledge how ICT is used in agrarian sector and why do we need to protect these technologies.

For the enterprises of the agrarian sector also mechanisms of state are important to develop the communication systems in a country. The research of necessity of forming the complex of measures of the state effect on the development of innovations, where communication systems play the role of the information distribution environment, required for provision of the innovative activity of the enterprises of the agrarian sector, was conducted by Granate, A. (2014).

Information technologies are important also in more efficient product placement of agro-sector products, e.g. using neuroscience, eye-trackers, etc. Consumer neuroscience is a phenomenon that has become an important tool of marketing management when defining customer driven strategies. The aim of consumer neuroscience (neuromarketing research) is a better understanding of the principles of decision-making and the strategy of customer and consumer behaviour in economic processes through neuroimaging and biometric methods, psychological and neurobiological concepts and knowledge (Berčík et al., 2016).

According to before mentioned researches the use of ICT in agrarian sector develops. But not only the use of these technologies is crucial nowadays to be competitive. Sufficient information security of these technologies and information assets must be maintained.

The term information security is often used in the relation to the information provided. Information security can be defined as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information (Whitman and Mattord, 2012).

The information security has become a complex managerial issue when following recent developments affecting the information security threat landscape. (Dor and Elovici, 2016)

Information assets are significant competitive and efficient sources of business in the globalizing knowledge economy. The significance of information security is therefore increasing (Mayadunne and Park, 2016).

It is difficult to define each level of information protection. Their vulnerability is on each level such as physical, organizational, procedural, personnel, management, administrative and also in terms of hardware and software (Oláhová, 2006).

Information security is not a management process that directly produces a profit, but it is a necessary prerequisite for direct profit making process. The aim of information security is to reduce the possibility of applying the threats and in case they appear it is to minimize their impact. Quality security management requires a combination of technical and business skills and knowledge of people, many of them are not intuitive. It is important to understand the information security as a complex process. Additionally, it is necessary to determine the correct security infrastructure, define the security policy and specially to analyse security risks (Hallová et al., 2017).

Also the analysis for security risks is important to provide knowledge of new dangers and threats for information assets, data and information systems. This analysis should be provided at regular intervals.

Analysis of security risks and their management is an essential tool in the hands of the senior management of the enterprise in order to protect investments in information systems, and thus to support the main business processes. Custom design of the risk analysis process can be distinguished by the details and depth of approaches to solve them. Based on the risk analysis, it is possible to specify the appropriate measures with regard to the identified threats (Hennyeyová, Tóthová, Hamášová, 2013).

Digital literacy is a necessity when we everyday use information technologies. This literacy or knowledge should not only by about how to use information technologies but also how to protect them and therefore the population must be taught about these technologies from childhood (Hosťovecký, Stubna, 2012).

With the topic of digital literacy of citizens also Polakovič et. al. (2016) deal with and their focus is on E-Government and E-inclusion. E-inclusion is a part of the process of social inclusion. Its aim is to create a European information society for all, as defined by strategic documents concerning the information society in the European Union.

2 Data and Methods

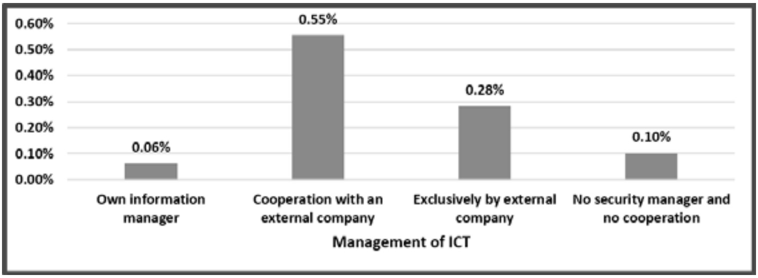
A questionnaire survey was conducted on granges of the Slovak Republic as a part of project KEGA (012SPU-4/2017) "Methodological manual processing

Enterprise security policy" for mapping the current information security in this sector. Aim of the research was mostly only on non-technical part of the information security – management of ICT in granges, management of security of ICT, risk analyses, security documents, staff awareness of security and threats to ICT, used security means in monitored granges. The survey was used in 149 granges in the Slovak Republic. Management of ICT points to who is responsible for ICT and IS – an internal employee; an internal employee and a cooperation with an external information company; the management of ICT is provided only by an external information company; the last opportunity of this question was that granges do not have management of their ICT. The second part was focused on the management of ICT security in granges with three possible options. Every grange provides some form of information security, whether by own employee or by external information security company. With the information security also risk analysis is related which means when granges provide risk analysis for information treats. This analysis must be provided when ICT/IS are used and granges work with sensitive data, e.g. wage data, personal information of employees, etc. The fourth part of the research focused on use of non-technical security means – security policy and security project – if granges use them, because granges also work with sensitive data of employees. Awareness of employees about information security and threats was the fifth part of research, because nowadays everyone must know the basics of information security because everyone of us uses information technologies also at home, not only in work. Perhaps the older generation does not as often as the younger generation. The last part of survey asks for used security means of ICT, information assets and property of granges.

3 Results and Discussion

Managing the information technologies in granges depends mostly on current employees who use them, because there are many job placements and not everyone uses these technologies for their daily work. Mostly the responsibility for these technologies is on the manager, in many cases on the chief economist. According to the research conducted on granges in the Slovak Republic the management of their information technologies is carried out by cooperation with an external company (55,47 %). Only 28,13 % of granges left their management of ICT exclusively on an external company and 6,25 % have their own internal employee – information manager. An alarming fact is that 10,16 % of granges do not have any ICT manager or do not cooperate with an external company. It is understandable that granges mostly cooperate with external companies when managing their ICT/IS, because it is more efficient from the economic view, e.g. lower costs for own information technician. These findings are necessary for further research of the information security of the agrarian sector in the Slovak Republic.

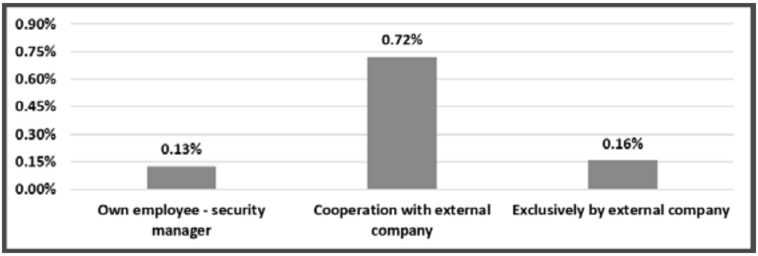
Figure 1 **Management of Information and Communication Technologies in granges of the SR**



Source: Own processing.

The way of managing information and communication technologies is closely linked to the security of these technologies. There are some interesting differences between the management of ICT and their security – the way granges are interested in this topic. From the Figure 2 it can be seen that 71,88 % of granges cooperate with an external company for security of their ICT. More internal employees are also included for the security of ICT in their own companies (12,50 %). 15,62 % of granges leave their information security on an external company and do not have an employee to care about their information security. The security of ICT is of the utmost importance when sensitive data are processed. Also granges work with this kind of data – wage data, accounting, personal information of employees, and many more. Good news is that granges care for their ICT security. Using of special security means is part of the last part of research.

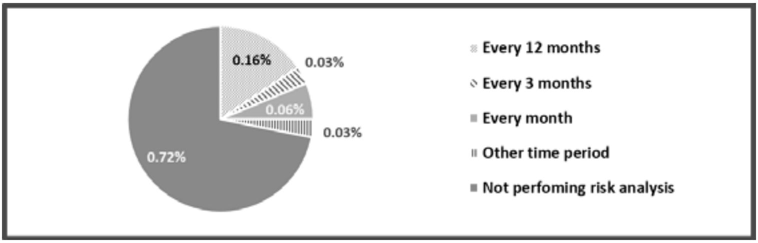
Figure 2 **Security of ICT in granges of the Slovak Republic**



Source: Own processing.

Although all granges ensure security of their information and communication technologies not all perform an analysis of potential security threats and risk for their ICT. An alarming 71,88 % of these granges do not provide this risk analysis. Risk analysis is important for a company to know which threats are dangerous for their data, information system or even for assets (not only information assets). This research focuses on information threats and therefore not providing a proper risk analysis for computer viruses, hacks, data and information thefts, etc. poses a serious risk to business data. Besides that, employees who are responsible for ICT/IS do not know how to protect or what security means do they have to use to protect their business data.

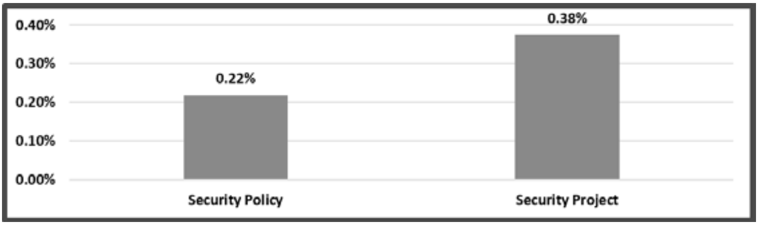
Figure 3 **Performing risk analysis for ICT**



Source: Own processing.

The risk analysis is directly connected with non-technical security means for protecting of ICT. These means are the security project and security policy documents. These documents contain the risk analysis to be performed in certain time intervals. The security policy contains ways of protection of ICT and IS as other assets as well as data flows of a specific company. However, the security policy and the security project are the basic security means for assets of a company, only small number of companies and even granges develop, applies and adhere them. The security policy document is a necessity for businesses which operate with sensitive data (as mentioned before). Mostly the responsibility for a security policy document has the chief economist of the grange. Or when a grange has a special employee for managing information technologies and their security, this person takes the responsibility to create, update this document and to familiarize employees with this document. This document contains basic information about the company (in this case a grange), information flows, who works with what form of data, what laws to follow, etc. When and information incident occurs this responsible person knows exactly who worked with the current technology.

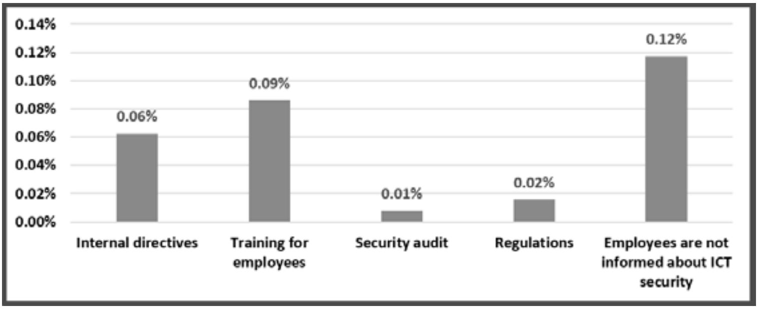
Figure 4 **Security policy and security project as basic non-technical security means**



Source: Own processing.

Last but not the least are employees and their knowledge of security and information risks. Just the low existence of security documents leads to these low rates of knowledge. But nowadays people use ICT not only at work but also at home. Therefore, each one must be careful about the information security and have the basic knowledge about information threats, risk and security. Each employee must come with this knowledge to his workplace even if he/she works with ICT or not. From the Figure 5 it can be seen that the awareness of ICT security and threats to ICT of employees in granges is at very low rate.

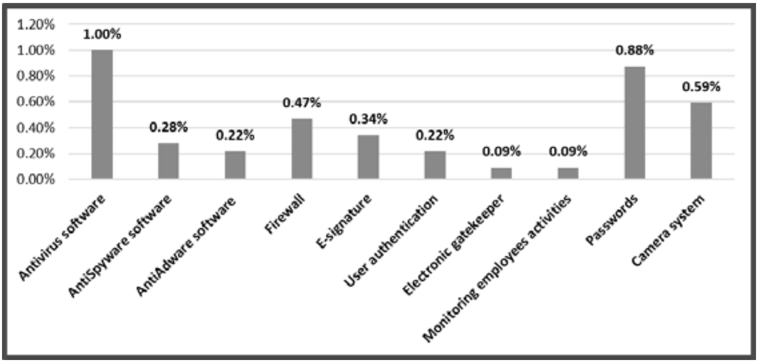
Figure 5 **Staff awareness of security and threats to ICT**



Source: Own processing.

According to research that granges do not use the non-technical security means in sufficient extent, the calming fact is that they use technical security means, e.g. antivirus software, firewalls, passwords, etc. Antivirus software (AV) is a necessity in each computer and nowadays in smart phones. It is the basic technical security tool to protect IT and IS. Mostly the AV software has a package of security means – firewall, antispyware, protection of internet banking when logging into it, anti-stealth protection and many others. It depends on current mark of the AV programme and financial resources of a company (grange). Other security means are mostly used for assets and information assets, e.g. computers, servers, etc. In very small numbers of granges electronic gatekeepers and employee monitoring are used. Use of passwords had to be used in every grange, but the number is lower – 87,5 %. It is strange, because in every grange they use computers and passwords are used not only for computer accounts but also when opening e-mail accounts. Also not every grange has a camera system to monitor the current area of a grange.

Figure 6 **Used security meansin monitored granges**



Source: Own processing.

4 Conclusion

According to the research it can be seen that the information security of granges in the Slovak republic is not on the highest level, but they do what they can according to their economic situation. It is important to have basically some technical protection means, e. g. antivirus software, etc. and a sufficient knowledge of IT security. Use of the non-technical protective means – security project and security policy, is also important, but there is hope in the future that these means will be used more often and some day in every grange of the Slovak Republic. In case that granges will exist in the future. The agrarian sector is important to ensure food security of each country and every country has to support this sector because food is priority of life.

Acknowledgements

This paper was created within the project KEGA (012SPU-4/2017) "Methodological manual processing Enterprise security policy".

References

1. BERČÍK, J., HORSKÁ, E., GÁLOVÁ, J., MARGIANTI, E. S. (2016). Consumer neuroscience in practice: The impact of store atmosphere on consumer behavior. *Periodica Polytechnica Social and Management Sciences,* 24(2), pp. 96-101.
2. DOR, D.,ELOVICI, Y. (2016). A model of the information security investment decision-making process, *Computers & Security*, Vol. 63, November 2016, p. 1-13. ISSN 0167-4048. DOI 10.1016/j.cose.2016.09.006.
3. GÁLA, L., POUR, J., TOMAN, P. (2006). Podniková informatika, Praha: Grada Publishing, 484 p.
4. GRANATE, A. (2014). Directions of the state effect on the development of communication systems of the agrarian sector enterprises. *In International Journal of Economics and Financial Issues*, Volume 4, Issue 3, 2014, p. 572-579.
5. HALLOVÁ, M., POLAKOVIČ, P., VIRÁGH, R., SLOVÁKOVÁ, I. (2017). Information Security and Risk Analysis in Companies of Agriresort, *AGRIS on-line Papers in Economics and Informatics*, Vol. 9. No. 1, pp. 49-55, DOI 10.7160/aol.2017.090104. Retrieved from http://online.agris.cz/archive/2017/1/4
6. HENNYEYOVÁ, K., TÓTHOVÁ, D., HAMÁŠOVÁ, K. (2013) „Actual situation of risk analysis in enterprises of agrosector in Slovakia", *8th International Conference on Applied Business Research (ICABR)*. Brno, 2013, pp. 238-244.
7. HOSŤOVECKÝ, M., STUBNA, J. (2012). Development of digital literacy in technical subjects at primary schools. ICETA 2012 – 10th IEEE International Conference on Emerging eLearning Technologies and Applications, Proceedings, art. No. 6418606, pp. 139-141. DOI: 10.1109/ICETA.2012.6418606
8. JAROLÍMEK, J., VANĚK, J. (2003). The intensity and quality of Internet usage in the agriculture sector and possibilities of its further development, *Plant, Soil and Environment*, Vol. 49, No. 11, pp. 525-529.
9. MAYADUNNE, S., PARK, S. (2016). An economic model to evaluate information security investment of risk-taking small and medium enterprises, *International Journal of Production Economics*, Vol. 182, pp. 519-530. DOI 10.1016/j.ijpe.2016.09.018.
10. MONTEGUT-SALLA, Y., CRISTÓBAL-FRANSI, E., GÓMEZ-ADILLÓN, M. J. (2013). Understanding the situation and factors of ICT adoption in

agricultural cooperatives. *In Journal of Electronic Commerce in Organizations*, Volume 11, Issue 3, July 2013, p. 1-26,

11. OLÁHOVÁ, E. (2006). Počítačová bezpečnosť, *Konkurencieschopnosť v EÚ – výzva pre krajiny V4 2006*: Medzinárodné vedecké dni. Nitra. Slovenská poľnohospodárska univerzita, pp. 1567-1570.
12. PAVLÍK, J., VANĚK, J., & STOČES, M. (2015). Software tools for movement visualization in agrarian sector. *In Agris On-line Papers in Economics and Informatics*, Volume 7, Issue 2, 2015, Faculty of Economics and Management, p. 68-76,
13. POLAKOVIČ, P., SLOVÁKOVÁ, I., HENNYEYOVÁ, K. (2016). E-Government as a reason for increasing digital literacy of citizens in the current concept of global e-democracy in the European Union. *In Globalization and socio-economic consequences 2016*, pp. 1761-1767.
14. WHITMAN, M. E., MATTORD, H. (2012). Principles of Information Security, United States of America: Boston, 601 p.