SECURITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES

BEZBEDNOST INFORMACIONIH I KOMUNIKACIONIH TEHNOLOGIJA

Kamil Boc
University of Zilina, Faculty of Security Engineering, Zilina, Slovakia

Zdenek Dvořák
University of Zilina, Faculty of Security Engineering, Zilina, Slovakia

Zoran Čekerevac
"UNION – Nikola Tesla" University, Faculty of Business and Law, Belgrade, Serbia

JEL Category: **C88, L86**

Abstract

With the development of computerization, information and communication technologies (ICT) are rapidly penetrating in all areas of human life. The state of information security and security of information systems is at a relatively low level. Threats and risks related to ICT by relevance and severity of possible consequences are most often directed at the state level, somewhat less towards banks, insurance companies, marketing and other companies that have larger amounts of personal data of users. However, small businesses and individuals are also very often exposed to the attacks. The authors analyze the legal environment in the IT sector of the Slovak Republic. After introductory considerations, the paper analyzes the legal regulations of the European Union and, in particular, of the Slovak Republic. The accent was placed on the security standards of the information systems of Slovakia. After that, the technical norms of relevance to the security of information and communication technologies are discussed. The authors dealt with long-term issues of security and the spread of good practice in the protection of property, information and communication systems. The aim of this article is to present the standard security and information systems of the European Union. Based on the research carried out, the authors point out that the goal of the academic environment should be to continuously find solutions to the new and emerging challenges that arise every day. One of the most difficult tasks is the transfer of this new knowledge into the legal framework and technical standards.

Keywords: *security, safety, information and communication technologies, standards, norms, Slovakia*

Address of the author:
Kamil Boc
kamil.boc@fbi.uniza.sk

Apstrakt

Sa razvojem kompjuterizacije, informacione i komunikacione tehnologije (IKT) naglo prodiru u

sve oblasti ljudskog života. Stanje sigurnosti informacija i sigurnosti informacionih sistema je na relativno niskom nivou. Pretnje i rizici u vezi sa IKT po značaju i težini mogućih posledica najčešće su usmereni ka državnom nivou, nešto manje ka bankama, osiguravajućim kompanijama, marketinškim i drugim kompanijama koje poseduju veće količine ličnih podataka korisnika. Međutim, napadima su izložena i mala preduzeća i vrlo često i pojedinci. Autori u radu analiziraju pravno okruženje Slovačke Republike. Posle uvodnih razmatranja, u radu se analizira zakonska regulativa Evropske Unije i, posebno, Republike Slovačke. Akcenat je stavljen na bezbednosne standarde informacionih sistema Republike Slovačke. U nastavku su prikazane tehničke norme od značaja za bezbednost informacionih i komunikacionih tehnologija. Autori su se u radu bavili dugoročnim pitanjima bezbednosti i širenja dobre prakse u zaštiti imovine, informacionih i komunikacionih sistema. Cilj ovog članka je predstavljanje standardnih sigurnosnih i informacionih sistema Evropske unije. Na osnovu izvršenih istraživanja, autori ukazuju na to da cilj akademskog okruženja treba da bude neprekidno pronalaženje rešenja novih i novih izazova koji se svakodnevno javljaju. Jedan od veoma teških zadataka je prenošenje ovog novog znanja u zakonski okvir i tehničke standarde.

***Ključne reči**: bezbednost, sigurnost, informacione i komunikacione tehnologije, standardi, norme, Slovačka.*

1 INTRODUCTION

The current development of the company is closely related to the development and modernization of ICT. In recent history, ICT has gradually begun to be used in science and research, military, aerospace, automotive, medicine and, in recent years, the arts and almost all areas of human life. (Cekerevac, et al, 2016) The aim of the researchers at the cooperating universities in Serbia and Slovakia was to gradually focus attention on the number of areas and problems of using ICT in life. Over the past 10 years, authors have been creating a series of articles focused on selected informatization issues (Cekerevac et al, 2016).

The main goal of our research is to shift knowledge into areas related to the use of ICT in human life. We keep learning the results of our research in the teaching of our subjects and present them at international conferences. Part of the research activity is cooperation on the creation of a legal framework in the national environment. The legal environment is generally divided into strategies, e.g. Informatization Strategy, Information Security Strategy, Public Administration Information Strategy (Slovak strategy documents, 2018), laws - e.g. the Act on the Protection of Classified Information, the Personal Data Protection Act (Legal frame of Slovakia, 2018) ordinances and technical standards (ISO27000, 2018).

2 LEGAL REGULATION OF INFORMATION SECURITY IN LAW OF EUROPEAN UNION AND SLOVAK REPUBLIC

EU, realizing the importance and significance of ICT system assets, inter alia, in its Directive no. 2008/114/ES recommended the ICT systems to become an individual sector of critical infrastructure and to subject to corresponding protection. SR in the act no. 45/2011 Coll. on the protection of critical infrastructure accepted this recommendation and listed ICT as an individual sector of critical infrastructure in SR under Ministry of Finances of SR. (EU directive 2008/114, 2018) and (Act no. 45/2011, 2018).

Security of ICT systems in SR is regulated in addition to Directive 2008/114/ES elaborated in Act no. 45/2011 Coll. on critical infrastructure, as well as by other legal and internal regulations, technical norms and international contracts it is bound to.

Other most important legal acts contain:

a. Directive of European Parliament and Council no. 2002/58/ES from 12th July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
b. Directive no. 95/46/ES of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with

regard to the processing of personal data and on the free movement of such data.

c. Act no. 215/2004 Coll. on the protection of classified information and related notices of NBU SR (notice of NBU no. 90/2002 Coll. on the security of technical devices, notice of NBU no. 91/2002 Coll. which establishes details of cryptographic protection of information).
d. Act no. 428/2002 Coll. on the protection of personal information.
e. Act no. 300/2005 Coll. criminal law.
f. Act no. 275/2006 Coll. on information systems of public administration and on amendments of certain acts.
g. Act no. 513/1991 Coll. commercial law.
h. Act no. 483/2001 Coll. on banks.
i. Act no. 324/2011 Coll. on post services and on the amendment of certain acts,
j. National strategy for information security in the Slovak Republic (UV no. 570/2008).
k. Decree of the Ministry of Finances of the Slovak Republic no. 312 from 9th June 2010 on standards for information systems of public administration (Legal frame of Slovakia, 2018).
l. Technical norms – regulating management and security of ICT systems (ISO/IEC 27000:2009, ISO/IEC 27001:2006, ISO/IEC 27002:2009, ISO/IEC 27005:2011, ISO/IEC 27006:2007, ISO/IEC 27008:2011, ISO/IEC 27011:2008, ISO/IEC 27799:2008, developed standards).

Ad a) Directive 2002/58/ES concerning the *processing of personal data and the protection of privacy in the electronic communications sector* harmonizes the regulations of member states required for providing of equal level of protection of basic freedoms and rights, especially right for privacy, with regard to processing of personal information in field of electronic communication and for providing of free movement of these data and electronic communication devices and services.

Ad b) Directive 95/46/ES of the European Parliament and of the Council on the *protection of individuals with regard to the processing of personal data and on the free movement of such data* obliges the member states to protect the basic rights and freedoms of persons, mainly their right for privacy regarding the processing of personal data. It binds the member states do not limit or obstruct the free flow of data between member states for reasons connected to their protection.

Ad c) Act no. 215/2004 Coll. *on the protection of classified information* defines terms and identifies classified information into four levels of confidentiality, determines organizations and units responsible for their protection, responsibilities, sanctions, which may be used in case of violation of law, determines the obligation to create security project, sets the security standards, etc. (Legal frame of Slovakia, 2018).

Ad d) Act no. 428/2002 Coll. *on the protection of personal data in information systems* has as its goal protection of basic rights and freedoms of persons during processing of their personal information. It establishes the term personal data. Under personal data, all data related to identified or identifiable person, with the person being identifiable directly or indirectly mainly based on identification number (birth registration number) or based on one or more characteristics or marks, which form its physical, physiological, mental, economic, cultural or social identity. It simultaneously determines rights and obligations of persons related to providing of personal data into information system and rights, obligations and responsibility of entities and persons, which partake on processing of personal data, sets rights and obligations of operators of information system, intermediaries and persons affected by providing of personal data from information system, regulates the position and scope of operation of the state supervision authority for protection of personal data in information systems and sanctions for violation of this law. It establishes the obligation to create a security project of the information system (Legal frame of Slovakia, 2018).

Ad e) Act no. 300/2005 Coll. *criminal law* defines subject matters of illegal actions related to the operation of the information system and its

assets. Illegal actions based on their subject matters may be divided into four groups:

1. crimes violating *protection of intellectual property*, competitive environment, trademarks and against fair competition,
2. crimes violating the *general protection of personality*,
3. *computer criminality* and computer piracy,
4. other crimes of *more general* nature, which may be related to a given field (endangering of state secret, economic secret, fraud, violation of the secrecy of messages, etc.) (Legal frame of Slovakia, 2018).

Ad f) Act no. 275/2006 Coll. *on information systems of public administration* and on amendment of certain acts as amended determines rights and obligations of persons liable in field of creation, operation, utilization and development of information systems of public administration, basic conditions for ensuring of integrability and security of information systems of public administration, administration and operation of central portal and process for issuing of electronic transcript of data from information systems of public administration and output from information systems of public administration. It introduces terminology, defining for example *information system, meta information system, cross-sectoral information system.* It introduces the term *liable persons* and their responsibilities, among which belongs the obligation to protect the information system of public administration from abuse. It introduces *standards*, which are a tool for providing integrability and security of information systems of public administration (Legal frame of Slovakia, 2018).

Ad g) Act no. 513/1991 Coll. *The commercial law* defines *trade secret* (Legal frame of Slovakia, 2018).

Ad h) Act no. 483/2001 Coll. *on banks*, defines *bank secret* (Legal frame of Slovakia, 2018).

Ad i) Act no. 324/2011 Coll. *on postal services* and on the amendment of certain acts defines *postal secret and protection of information and personal data* (Legal frame of Slovakia, 2018).

Ad j) National strategy for information security in SR. Its goal is to create a basic framework of information security of SR. The strategy contains the background, competence-based distribution of competencies, a proposal for direction, priorities, and steps for reaching of a set goal. Part of this document is also a basic description of individual tasks with the goal to provide security for the whole digital space of SR, except for the classified information sphere. This contains mainly the measures against information leak and their unauthorized use, integrity breach of data, violation of citizen rights for protection of personal information, protection from damage and abuse of information and communication systems, damage to reputation of state and private institutions, as well as measures for enforcement of relevant law norms of SR and European Union.

Ad k) Decree of the Ministry of Finances of the Slovak Republic no. 312 from 9th June 2010 *on standards for information systems of public administration*. The decree determines standards for information systems of public administration, security standards.

3 SECURITY STANDARDS OF INFORMATION SYSTEMS IN SLOVAK REPUBLIC

Elements of an information system (hereinafter “IS”) itself have significant importance for society as a whole. (Prigoda, et al, 2015) National executives are aware that failure of IS would have unforeseeable consequences and would complicate the administration of public issues. It is a similar situation with private entities that use ICT for their entrepreneur activities. For example, the banking sector would, in case of failure of information systems, now only bankrupt, but would also significantly endanger the operation of the national economy. That is why it is necessary to create the standards for protection within public administration. For the purposes of this work, generally, binding legal acts that regulate IS security in conditions of public administration shall be analyzed further on.

In conditions of SR, the security standards for public administration IS are based on the Decree of the Ministry of Finances of the Slovak Republic no. 312, and they regulate (Slovak strategy documents, 2018) (Legal frame of Slovakia, 2018):

3.1 Management architecture

a) Information security management – the standard is:

- creation, approval, realization, and compliance with the security policy of liable person,
- selection of person or persons responsible for information security of all information systems of the liable person of public administration in compliance with security policy,
- ensuring of coordination of activities of organizational units of the liable person while addressing the information security,
- determination of specific responsibility for individual assets of the liable person,
- determination of security positions in information systems of public administration, determination of security requirements of individual positions, determination of incompatible positions; security positions consist mainly of the system administrator, operator, auditor, and programmer.

b) Personnel security – a standard for the personnel security is:

- ensuring all employees are instructed about security policy, their duties, and rights resulting from it, about responsibilities before they gain access to the information system of public administration, and that these are listed in his work contract,
- ensuring the responsibility of employees to be informed about security incidents,
- creation of a process for disciplinary action related to persons which violate the security policy of the liable person or any of the related regulations,
- creation of a process for ending of employment of own employee, and ending of cooperation with an external employee or third party.

c) Risk management for the field of information security – the standard is:

- implementation of a system for management and monitoring of risks related to information systems of public administration,
- utilization of system for management and monitoring of risks for all processes of information security management,
- identification, analysis, and evaluation of risks connected to the use of assets and information systems outside of spaces of liable person and the introduction of adequate procedures and measures for reduction of these risks,
- analysis of processes important for activities of the liable person from the viewpoint of their dependency on information systems, and determination of processes that cannot continue in case of outage or limitation of the functionality of information systems of public administration; these processes are called *critical processes,*
- analysis of risks resulting from threats to information systems of public administration, on which the critical processes depend; these information systems are *critical information systems* of the public administration,
- creation of plans for restoring of non-functional, damaged or destroyed critical information systems of public administration.

d) Information security management control mechanism – a standard is:

- compliance of security policy of liable person and provision and execution of internal control or audit of information security, whose periodicity is determined by the security policy of liable person,
- provision of archivization, protection, and evaluation of audit reports.

3.2 Minimal technical provisions

a) Protection against malicious software – a standard is:

- protection in the scope of control of incoming electronic mail for the presence of malicious code and unallowed types of attachments, detection of the presence of malicious code, check of files received or sent from the internet for the presence of harmful software, detection of the presence of malicious code on all websites of liable person,
- introduction of protection from unsolicited e-mail (spam),
- use of only legal and allowed software,
- setting rules for downloading of files through external networks,
- support for ensuring of authenticity and integrity of files through the use of cryptographic devices, especially the electronic signature,
- support for the encryption of electronic documents (ISO 27000, 2018).

b) Network security – a standard is:

- ensuring of protection of the external and internal environment through tools of network security (firewall),
- keeping records on all connection points of the network, including connections to external networks,
- ensuring that the internal act of access management is created for each connection between these networks (ISO 27000, 2018).

c) Physical security and environment security – the standard is:

- locating the public administration information system in such space, that the information system or at least its vital components are protected from negative natural influences and environmental influences, possible accidents of the technical infrastructure and physical access of the unauthorized persons (protected area),
- separating the protected area from other spaces by physical devices, especially by walls and barriers,
- ensuring that in the surroundings of the protected area are no facilities such as sewage, waterworks or materials, mainly flammable, which could represent a threat to public administration information system located in the protected area,
- creation and implementation of rules for work in the protected area,
- providing protection from power supply outage and ensuring that such outage shall not occur,
- ensuring that the existing backup capacities of the information system are located in the secondary protected area, sufficiently remote from the protected area,
- ensuring that the operation, use, and management of information system is in accordance with specific regulations, internal regulations and its contractual obligations,
- creation, introduction and control of commitment to rules for maintaining, storing and evidence of technical components of the information system, use of information system devices for other purposes than originally intended, use of devices of information system outside of determined spaces, deletion, decommissioning and disposal of information system devices and all types of relevant backups, transport of technical components of information system outside spaces of liable person, handling of electronic documents, system documentation, memory media, input and output data of information system in such way, that their unauthorized publishing, removal, damage or modification is prevented,
- determination of parameters that define the maximum time period for an outage of information system and creation and the introduction of measures, which are focused on solving of the restoration of operation in case of information system outage (ISO 27000, 2018).

d) Software updates – standard for software updates are:

- providing of update of versions of protective software, including protecting all other components and connected devices,

- performing of update at least in compliance with security policy (ISO 27000, 2018).

e) Monitoring and management of security incidents – the standard is:
   - creation of internal act containing the procedure for reporting of security incidents and revealed vulnerable points of information systems, the procedure for solving of individual types of security incidents and method of their evaluation, a method of evidence of security incidents and used solutions,
   - ensuring that all users of an information system are informed on an appropriate way about procedures, and to ensure these rules are observed,
   - introduction of registration of all outages of information system and methods of their solving,
   - use of intrusion detection system,
   - creation and operation of contact point for reporting of security incidents and revealed vulnerable points of information systems (ISO 27000, 2018).

f) Periodical evaluation of vulnerability – a standard is a periodical evaluation of vulnerable points and threats to information system identified in accordance with the security policy of the liable person with a periodicity of at least once per year (ISO 27000, 2018).

4 SECURITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN TECHNICAL NORMS

Information security is in addition to generally binding legislation regulated also by technical norms. The scope of these norms is within all EU states and a demand exists to implement these into the protection of all IS. The affected norms regulate procedures and measures which should ensure achieving of security standards of IS within EU.

Among the most important of technical norms in this field belongs (ISO 27000, 2018):

a. ISO/IEC 27001 – *Information technologies – Security techniques – Systems of Information Security Management - Requirements*. It is the main norm for a system of information security management. This international norm covers all types of organizations (e.g. commercial companies, government agencies, non-profit organizations). It is a complex system of information security management from realization, maintaining and enhancing the system of information security management in every organization without regard to its size. It addresses also the character of contractual relations for information security in business connection, as well as contractual relations in maintenance and service for the processing of sensitive information.

b. ISO/IEC 27002/C1 – *Information technology. Security techniques. Code of practice for information security management.* This international norm introduces guidelines and general principles for initiation, implementation, maintaining and enhancing information security management within the organization. It provides a general manual of recognized goals of information security management. It contains procedures for control of goals in following spheres of information security management.

5 CONCLUSION

The article presented a vision of security of information and communication technologies. The authors address the issue in the long term and aim to spread good practice in the protection of assets, information and information systems.

In recent years, we have seen the data backup and archiving as a basic problem with ICT. Experience from major incidents and natural events often resulted in a complete loss of data and information.

Modern ICTs, such as cloud computing, create options for their proper backup and archiving. On the other hand, the likelihood of their misuse, damage and loss increases.

The big challenge today is data mining from all electronic sources. The gradual penetration of the Internet of Things and the Internet of Everything brings a whole host of challenges and challenges.

Our goal is to educate students who choose their security and information and information systems

for lifetime work. This area of human work is very promising and well paid.

The goal of the academic environment is to permanently explore new and new challenges that need to be addressed. The difficult task is to transfer this new knowledge into the legal framework and technical standards.

WORKS CITED

Act no. 45/2011 Col. of critical infrastructure (2018, September 2018) http://www.zakonypreludi.sk/zz/2011-45 in Slovak,

Cekerevac Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2016) Big vs small data in micro and small companies. *Communications: scientific letters of the University of Žilina*, *18(*3), p. 34-40. ISSN 1335-4205.

Dvorak, Z., Leitner, B., & Mocova, L. (2016) *The need for education in the field of security management and critical infrastructure protection.* Menadžment 2016: međunarodna naučna konferencija : zbornik rezimea : Beograd, Srbija, ICIM plus, ISBN 978-86-6375-053-1. p. 185-187.

European Union directive no. 2008/114 ES *(2018, September 2018) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN*

ISO 27000. *(2018, September 2018) https://www.iso.org/isoiec-27001-information-security.html*

Legal frame of Slovakia *(2018, September 2018) http://www.informatizacia.sk/legislativa-sr/684s*

Prigoda. L., Cekerevac, Z., Dvorak, Z. & Cekerevac, P. (2015, Apr 19) *One look at modern information security. Sustainable Development of Mountain Territories*, *4*(22) (2014), p. 99-103. ISSN 199B-4502.

Slovak strategy documents *(2018, September 2018) http://www.informatizacia.sk/strategicke-dokumenty-is/600s*

This publication was created thanks to supporting under the R & D project for the project:

Centrum excelentnosti pre systémy a služby inteligentnej dopravy II., ITMS 26220120050 co-funded by the European Regional Development Fund.

"We support research activities in Slovakia / The project is co-financed from EU sources"