KOŠICKÁ BEZPEČNOSTNÁ REVUE

KOSICE SECURITY REVUE

Vol. 10, No. 2 (2020), p. 171 – 184

ISSN 1338-4880 (print ver.), ISSN 1338-6956 (online ver.)

Analysis of the information environment in healthcare organizations in terms of information security

Analýza informačného prostredia v zdravotníckej organizácii z pohľadu informačnej bezpečnosti

Miroslav TOMŠŮ[1]

[1] *Faculty of Applied Informatics, Tomas Bata University in Zlín*

The manuscript was received on 27. 10. 2020 and was accepted after revision for publication on 03. 12. 2020

Abstract:

Information as an asset is an important part of an organization's operations. The value of information is receiving increasing attention. In addition to the traditional trade in products and services, information is becoming a commodity. The latest information processing technologies bring not only benefits but also threats.

The article discusses and explains the information environment in the organization and defines vulnerability. The research describes the share of the use of paper and digital forms of the information environment. It examines the environment in which stored information is located and its security. It determines the security of the information environment against the leakage of sensitive information - awareness of employees in the field of information security, authorization of individual employees and their implementation, and ensuring a digital user environment.

Keywords: *information security, vulnerability, threat, healthcare.*

Abstrakt*:*

Informácie ako aktívum predstavujú dôležitú súčasť chodu organizácie. Hodnote informácií je venovaná stále väčšia pozornosť. Informácia sa stáva vedľa tradičného obchodu s výrobkami a službami, komoditou. Najnovšie technológie, spracovávajúce informácie prinášajú nielen úžitok, ale aj hrozby.

Článok pojednáva a vysvetľuje informačné prostredie v organizácii a definuje zraniteľnosť. Výskum popisuje podiel využívania listinnej a digitálnej formy informačného prostredia. Skúma

prostredie, v akom sa uchovávané informácie nachádzajú a ich zabezpečenie. Zisťuje zabezpečenie informačného prostredia pred únikom citlivých informácií - povedomia zamestnancov v oblasti bezpečnosti informácií, oprávnenia jednotlivých zamestnancov a ich vykonávanie, a zabezpečenie digitálneho užívateľského prostredia..

Kľúčové slová: *informačná bezpečnosť, zraniteľnosť, hrozba, zdravotníctvo*.

Introduction

Healthcare organizations and their information environment are exposed by security threats from a variety of sources, including computer fraud, espionage, sabotage, vandalism, fires and floods. The source of damage is the information and communication technologies used and human resources, ie people, employees of the organization. They are becoming more common, their danger and sophistication growing. The question is how successful these threats can be implemented as an information environment vulnerable.

1. Information environment

The information environment is an integral part of the social environment and its structure, determined by basic social levels, consists of the human factor, which is the originator, mediator and user of the communication process, as well as the information and communication processes themselves. certain information flows and various information products are created, and all this is ensured by a certain material and technical base, which consists of information institutions, libraries, but also information technology and computer technology.

Finally, it is necessary to take into account the spatio-temporal dimension, which determines the direction, speed, addressability or novelty of the communicated information. Today, there is perhaps no need to discuss that the most important element of the information environment is the person with his cognitive and social aspects of personality, who represents the individual information environment. [1]

Information environment can be defined: Aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. Information environment is a heterogeneous global environment where humans and automated systems observe, orient, decide, and act on data, information, and knowledge. [2]

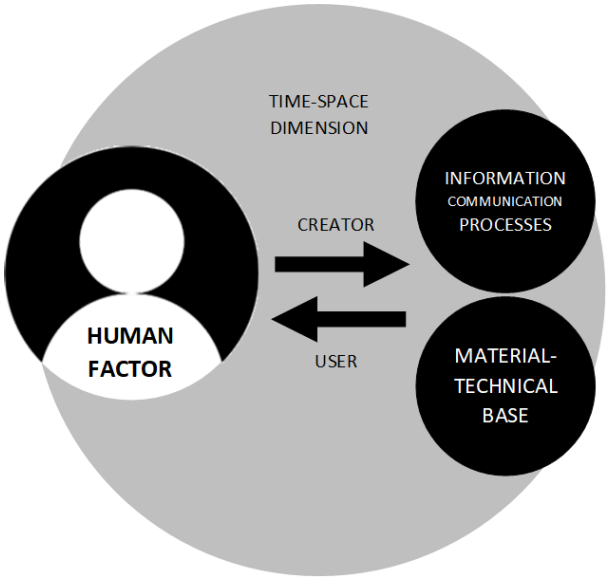

Fig. 1 Information environment model [Source: Author]

The information environment is a construct based upon the idea that the existence and proliferation of information and information systems creates a distinct operating dimension or environment. As a combination of tangible (physical information systems and networks) and intangible elements (information and decision-making), the information environment a resource for decision making and through for organization management. [3]

1.1. Vulnerability of the information environment

A vulnerability can be defined as a weakness of the environment that can be used by attackers to gain unauthorized access to the information environment or to perform unauthorized actions. Vulnerabilities can allow attackers to break into a file cabinet, access computer system memory, install malware, and steal, destroy, or modify sensitive data. In order for an attacker to exploit a vulnerability, he must be able to enter the information environment. Vulnerabilities can be exploited by various methods.

Vulnerability is a property where a reference object (environment) loses its ability to perform its function. As such, it means the action of external harmful effects - threats and reducing the degree of resistance to these threats. It can be not only parts of the protection system that do not reach the required level of security and thus become an easy and easily overcome element. A vulnerability is a place where a harmful effect penetrates and causes damage to the assets of a reference object.

A vulnerability with at least one known working attack factor is classified as an exploitable vulnerability. The vulnerability window is the time from the moment the vulnerability was introduced to the fix. [4, 5]

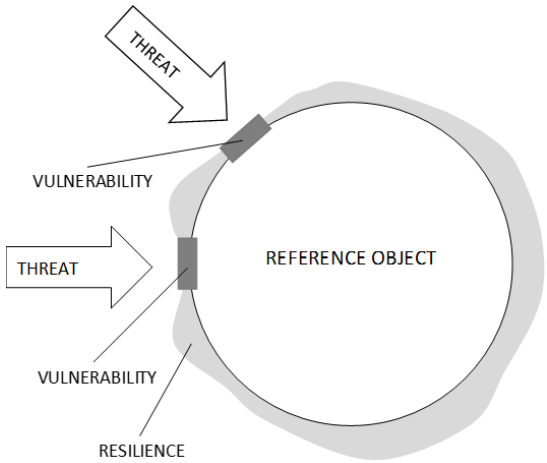

Fig. 2 Vulnerability of the reference object [4]

The vulnerability assessment of a reference object is usually performed in those places that are the least resistant to threats.

The most common causes of reference object vulnerabilities include the omission of a threat where a process or protection is malformed due to an error or an intentionally poor protection design, usually by the manufacturer (repeating code and spreading mallware to retrieve user data). Ignorance of the threat can also cause a vulnerability. The protection of the reference object is not ready for such an attack. A new form of harmful effect can also be defined as the cause of vulnerability, which most often causes damage during ineffective old protection or protection processes. [5]

2. Analysis of the information environment - research in a healthcare organization

The information system in a healthcare organization is a set of applications that serve to support medical procedures as well as the storage, modification of data and their transfer between employees. We understand the information system in the organization as a living organism, which consists of many dimensions (people, technical means and methods), each of which affects its quality.

The main objectives of the questionnaire survey were to obtain an overview of the organization's information environment, its use, staff training, and the provision of an information system, documents and communication.

The aim of the questionnaire survey was:

- *Find out to what extent and in what form the information environment is used in the medical facility,*
- *reveal whether medical staff are trained in the use and security of digital technologies,*
- *show ways to ensure internal communication between staff,*

– *Find out which of the healthcare professionals can access the patient's medical records / daily records.*

2.1. Composition of respondents

People, as one of the dimensions, use data and methods to process data and create an information and knowledge base of the organization, which serves as a basis for management, decision-making and administration of the agenda.

The questionnaire survey was conducted using a questionnaire, which was divided into several topics according to kinship. According to the discretion, only closed questions were chosen, which made the questionnaire easier for the respondents. The following target groups have been defined within the health department:

– *general nurse*
– *practical nurse*
– *orderly*

The predefined answer options in the questionnaire are the result of previous meetings and personal inquiries.

3. Results of a questionnaire survey

The results of the questionnaire survey are arranged according to individual questions and the answers of the respondents are arranged in tables for clarity, expressed in number and percentage and graphically represented by graphs.

3.1. Proportion of use of paper / digital form of information environment

Tab. 1 Proportion of use of paper / digital form of information environment [Source: Author]

Answer	Number	Percen
paper form	13	62 %
50: 50	8	38 %
electronic form	0	0 %

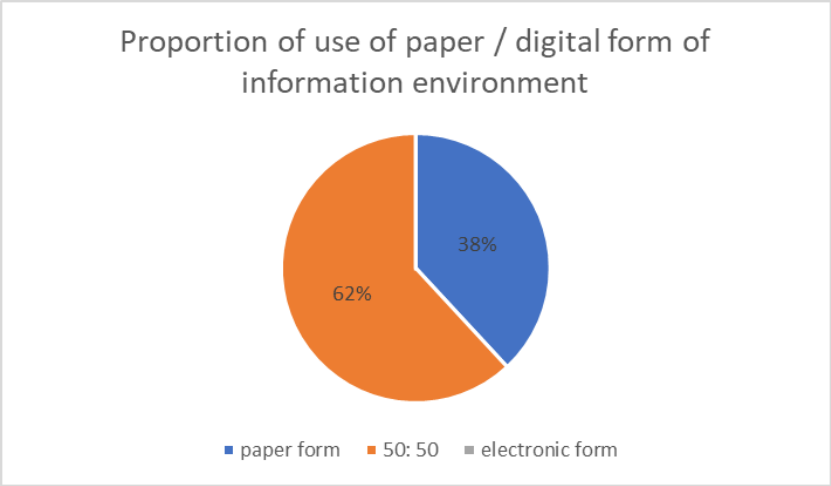

Fig. 3 Proportion of use of paper / digital form of information environment

[Source: Author]

Evaluation: At present, in the practice of many organizations there is a great trend to promote the so-called paperless offices, where, together with the popularity of cloud solutions, there is also pressure to maximize the digitization of all documents.

Most respondents stated that the use of the paper form of the information environment was predominant. A minority of respondents then chose the same share of paper and electronic forms of using the information environment as the same. Respondents are not convinced that the information environment is kept in electronic form. This points to the fact that staff either cannot work with information in electronic form or the organization has not yet carried out a fully electronic transformation.

3.2. In what form do you most often work with information?

Tab. 2 The form most often works with information [Source: Author]

Answer	Number	Percen
written	21	95 %
pictorial	1	5 %
brands, codes	0	0 %
sound	0	0 %

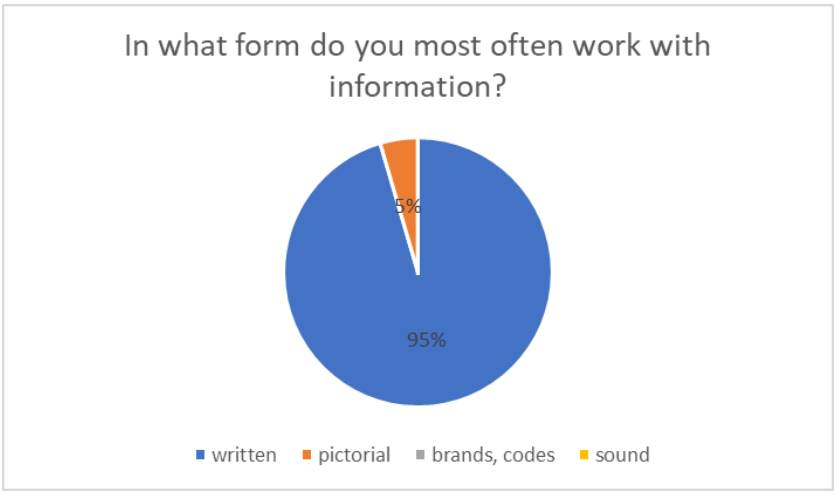

Fig. 4 The form most often works with information [Source: Author]

Evaluation: The overwhelmingly predominant written form of work with information points to the possibility of non-performed electronic transformation or obsolete devices that do not even provide outputs in electronic form.

3.3. Have you completed education focused on the use of digital technologies?

Tab. 3 Education focused on the use of digital technologies [Source: Author]

Answer	Number	Percen
no	14	67 %
yes, no later than the last year	3	14 %
yes, one to three years ago	0	0 %
yes, earlier than three years ago	4	19 %

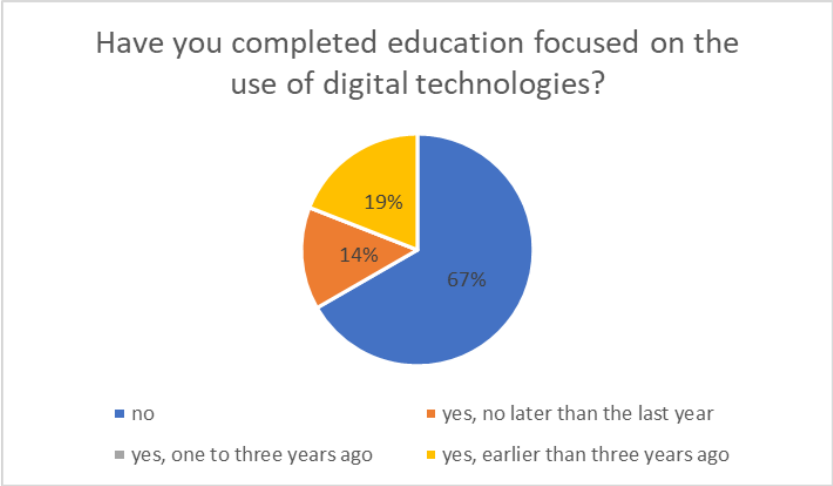

Fig. 5 Education focused on the use of digital technologies [Source: Author]

Evaluation: Education is the best way to use digital technologies to benefit the running of the organization. The prevailing negative answers to the completion of education focused on the use of digital technologies reflect the prevailing previous answers, where it exceeds the use of the paper form of the information environment. The staff is thus not familiar with all the possibilities of the information system in digital form and do not use it. Consistent answers belong to a minority, but show an effort to increase the share of digital technologies.

3.4. Have you completed digital security education?

Tab. 4 Digital technology security education [Source: Author]

Answer	Number	Percen
no	19	90 %
yes, no later than the last year	1	5 %
yes, one to three years ago	1	5 %
yes, earlier than three years ago	0	0 %

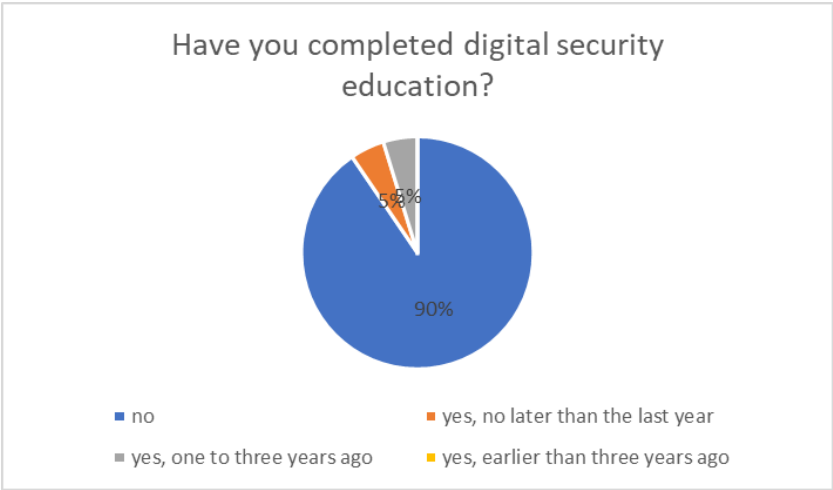

Fig. 6 Digital technology security education [Source: Author]

Evaluation: Security is considered a major challenge in the digital world. Dissenting answers to the question of whether staff are trained in digital security is an almost real threat. Staff are not sufficiently aware of the potential threats to the use of digital technologies in their jobs, although they are used sparingly, and can ultimately cause irreversible damage.

3.5. Does your password contain…?

Tab. 5 Content of password for the hospital information system [Source: Author]

Answer	Number	Percen
at least 16 characters	3	8 %
combination of numbers	13	35 %
combination of symbols	4	11 %
combination of lowercase letters	6	16 %
combination of capital letters	11	30 %

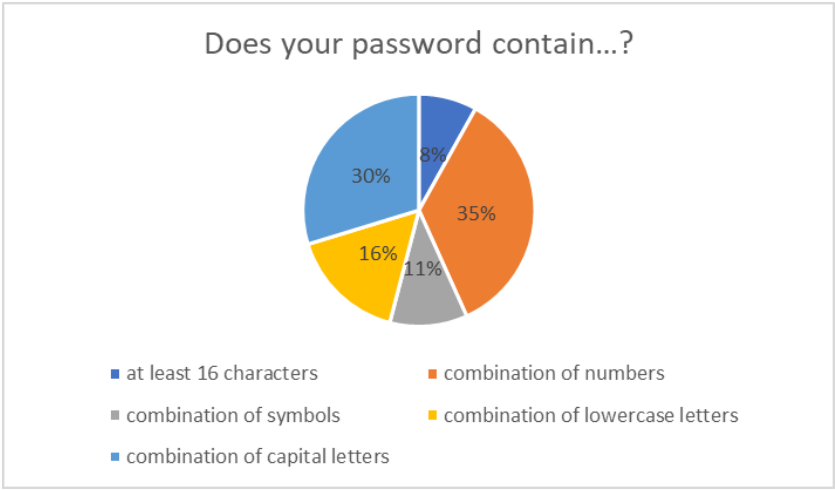

Fig. 7 Content of password for the hospital information system [Source: Author]

Evaluation: A strong password helps keep personal information safe, protect e-mails, files and other content, and prevent third-party users from breaking their account. The content of staff passwords according to the results of the submitted question of typical criteria in most cases contains only a combination of numbers, then a combination of capital letters. To a lesser extent, it is already a combination of lowercase letters and at least in passwords the staff combines special characters. To a small extent, passwords also reach a length of 16 characters. The threat of password cracking is so real.

3.6. Do you use different passwords for different services?

Tab. 6 Using different passwords for different services [Source: Author]

Answer	Number	Percen
yes	6	29 %
no	15	71 %

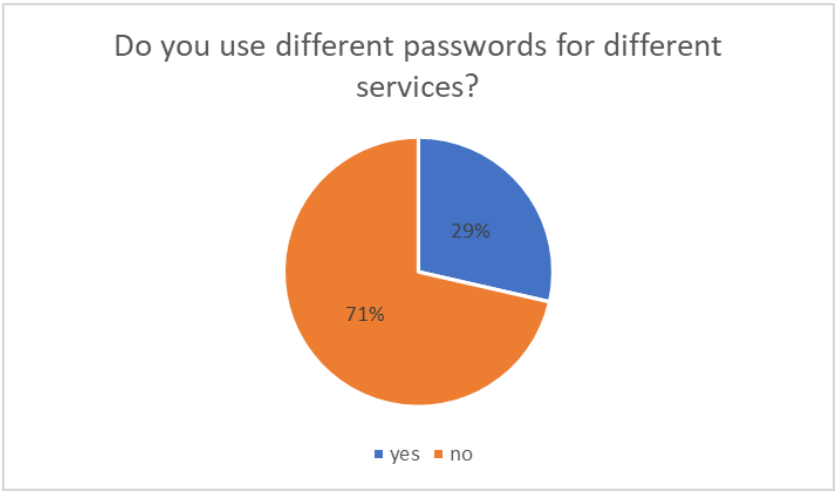

Fig. 8 Using different passwords for different services [Source: Author]

Evaluation: Creating strong and unique passwords for each user account is almost impossible, so people enter weak, easy-to-remember passwords or use the same passwords for multiple accounts. This was also confirmed by most of the staff of the medical organization. However, doing so poses a threat, especially when they use the same passwords for their private and work user accounts.

3.7. Have you ever provided someone with your login password?

Tab. 7 Providing a login password for a user account to another person [Source: Author]

Answer	Number	Percen
yes	3	24 %
no	18	86 %

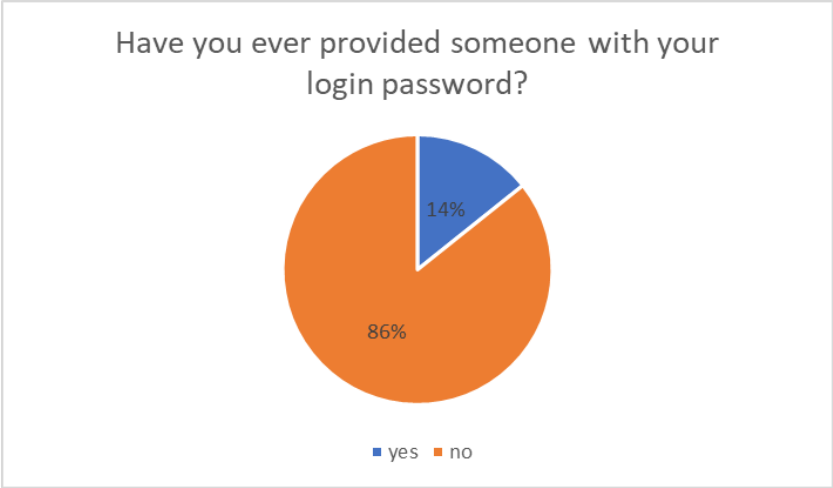

Fig. 9 Providing a login password for a user account to another person [Source: Author]

Evaluation: Sharing access to whatever services is a dangerous affair. Although only a minority of respondents answered, this is a real threat. Sharing and revealing a password is "secure" only to the extent that we trust the person and their ability to handle sensitive data. The ability should not be optimally equal to the ability to forget a piece of paper with a login name and password somewhere. Such cases should not occur at all in the case of an organization where staff process personal data.

3.8. Discussion of results and recommendations

From the above research we can find out that the share of the use of paper and digital forms of the information environment in a healthcare organization is almost the same. In a minority of cases, respondents answered that they work only with the paper form of the information environment. This is closely related to the technologies used in the healthcare organization. Most medical devices do not support digital outputs. These are analog devices that are not connected to a digital network. A local survey found that these devices are obsolete and it is absolutely necessary to unify the standardization of devices and connect them to the internal network.

As stated by the respondents in another question, which dealt with the form of information that employees work with, the paper form prevailed. This may be due to the fact that employees do not even have access to the information in digital form. This is because medical devices do not provide a digital interface. The digital transformation in healthcare organizations is not completely completed and its gradual implementation is very slow, compared to other organizations.

In two questions, respondents answered questions related to digital education and digital security education. Training in the use of digital technologies takes place according to the results of newly hired employees. However, others replied that they had not received any education in the use of digital technologies. According to the results of the healthcare organization, training focused on the security of digital technologies does not take place at all. A small percentage of respondents said they

had completed their education, but in a different way than in this health care organization. Education, especially on the security of digital technologies, is very important, especially for older users of the digital information environment.

When asked about the content of the for the hospital information system, most users answered that they use numbers or a combination of capital letters. This proves that users have at least a small security awareness. Although most respondents said they do not pass on their password to another person and do not use a single password for multiple services, a smaller percentage of employees are alarming. This is evidenced by the fact that employees lack training in the security of the use of digital technologies. The healthcare organization should introduce at least basic education in this area.

Conclusion

The growing use of ICT and modern technologies in healthcare, of course, presupposes the sharing of patient information between different healthcare facilities and their systems. This is almost impossible without digitization. The results of the questionnaire survey show that keeping a paper form of documentation strongly predominates in the medical facility. One possible cause is also outdated instrumentation that simply does not support digital outputs.

Innovation in healthcare, supported by information and communication technologies, helps doctors and patients alike. However, the problem of their wider implementation does not have to be just a lack of funds. As part of the questionnaire survey, 21 respondents participated in the research, which represents all the staff of the department of the medical organization. The questionnaire survey showed that the staff of the chosen health organization shows major shortcomings in digital literacy and security of digital technologies.

The security of personal data is undoubtedly a key issue to be addressed in the digital transformation of healthcare. The approach of medical staff is most important. However, the results show that employees choose weak, easy-to-remember passwords or use the same passwords for multiple accounts. Research has also shown that some share their access data with others.

Acknowledgment

This work was supported grant project IGA/FAI/2020/005 „Identification and analysis of the information environment of the organization in terms of cyber security" solved in 2020.

References

Books:

[1] SEDLÁČKOVÁ, Beáta. *Current information environment and information literacy*. ITlib. Informačné technológie a knižnice. Bratislava: Bratislava, 2011, (3). ISSN 1335-793X.

[2] *Department of Defense Dictionary of Military and Associated Terms: Joint Publication 1-02*. Washington: United States Navy, 2016.

[3] POŽÁR, Josef. *Fundamentals of information security theory*. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.

[4] LUKÁŠ, Luděk. *Theory of Security I.* Zlín: Radim Bačuvčík - VeRBuM, 2017. ISBN 978-80-87500-89-7.

[5] FOREMAN, Park. *Vulnerability Management.* 2st Edition. Broken Sound Pkwy NW: Auerbach Publications, 2019. ISBN 978-1439801505.

Author:

[1]**Miroslav TOMŠŮ –** Faculty of Applied Informatics, Tomas Bata University in Zlin, Nad Stráněmi 4511, 760 05, Zlin, Czech Republic, email: tomsu@utb.cz