The Impact of User Training on the Security of Information and Telecommunication Systems of the Police Force in the Slovak Republic[1]

Vincent Holubiczky[2]

This scientific study summarizes knowledge about information security and provides an introduction to the empirical part of the paper. It focuses on our own research via questioning respondents from the environment of the Police Force in the Slovak Republic. We focus mainly on frequency and purpose of using modern technologies at work and their often dangerous habits. We also deal with the impact of user training on the security of information and telecommunication systems. Additionally, examining the technical state and outdatedness of hardware and software, we deal with frequency and purpose of using modern technologies at work.

Keywords: security technologies, human factor, password management, information systems, training, security incidents

I. Introduction

We live in a digital age with an extreme amount of different technologies that we use in our daily lives. It is no different even in these times, when almost the whole world and many countries are paralyzed by the coronavirus pandemic - COVID19 and the war conflict in Europe. Because of these threats to our health and lives, in many cases work duties have been moved to the online space.[3]

Information security immediately became the center of attention. This fact is related to the rapid development of new and modern technologies that enable both simple and more demanding users to use electronic services, connect them, and thus create complex systems, which then place high demands in terms of functionality and efficiency.[4]

It is important to realize that this way of performing work duties creates risks due to leakage and loss of sensitive information. In addition, at home it can often be tempting for users to mix private matters with work duties. The so-called "Internet of Things" today offers such possibilities of the online space that we would not have expected a few years ago.[5] The ubiquitous technology and online environment in our daily lives make us less sensitive to potential threats and vulnerabilities.[6]

[1] This paper is linked to the solution of the partial task „Internet of Things“ of scientific research VÝSK. 245 „Modern technologies in committing, detecting, documenting, proving and preventing criminal activity, while ensuring public order and road traffic safety“, registered at the Academy of the Police Force in Bratislava..

[2] mjr. Ing. Vincent Holubiczky, PhD., assistant professor, Academy of the Police Force in Bratislava. E-mail: vincent.holubiczky@akademiapz.sk, orcid.org/0000-0002-6674-6476

[3] Vincent Holubiczky, *Moderné technológie a účel ich využívania*.In Projustice (Bratislava: Projustice.sk, 2020).

[4] Vincent Holubiczky, *Frekvencia využívania moderných technológií Policajným zborom.* (Bratislava: Akadémia Policajného zboru v Bratislave, 2020), 163-171.

[5] Vincent Holubiczky, *Prítomnosť hrozieb a zraniteľností pri využívaní informačných technológií. In: Policajná teória a prax* (Bratislava: Akadémia Policajného zboru v Bratislave, 2020), 5-19.

[6] Vincent Holubiczky, *Moderné technológie a účel ich využívania*. In Projustice (Bratislava: Projustice.sk, 2020).

In this article, we have decided to present the partial results of our research regarding security in relatively common activities within the work of users with telecommunication and information technologies used in the private sector and by members of the Police Force in the Slovak republic. Under the term information technology, or communication technology is usually understood as a set of techniques, procedures and means that human society uses to communicate information. From this point of view, the most important communication technologies include language, writing, letterpress, telephone, radio, television and, of course, the computer.[7] This is where information and telecommunication systems come into contact with security. Among them we can clearly include not only computers, but almost all elements and means of the modern world. Many terms are related to this issue, such as security, threat, risk, information, data and others. There are a large number of threats in the online space, while they are aimed not only at the vulnerability of technical equipment, but also to a considerable extent at people, the users of these systems and their subjective perception of security threats.

The relationship between threats and security is described by many authors, among whom Rak, in collaboration with Kopencová and Kolitschová, is intensively devoted to this topic.[8] Security is an extremely complex and multidimensional phenomenon that includes a large number of areas and disciplines - social sciences, natural sciences, but also technical, where informatics is an inseparable part. Each discipline perceives security according to its theory, practice, focus, knowledge and experience.[9] We can divide the threats according to different criteria, but as far as our issue is concerned, when using modern technologies, the most frequently present are "technogenic" and "sociogenic" areas, the source of which is human.[10]

The security of an information system means the ability of a network, or an information and communication system, to withstand, with a certain degree of reliability, accidental events or intentional actions that threaten the availability, integrity and confidentiality of stored or transmitted data or related services provided through this network and information system or accessible through this network and information system.[11]

With the development of technology, the concept of information security gradually became known. Data and information were no longer kept only in physical form in archives, but gradually moved to electronic form. There is an incalculable amount of data in the world. The basic difference between these data and information is that while the data contains some value, a fact, neutral for us, the information has a certain added value (negative or positive) for the given person or institution. Storing information in electronic form is at first glance a very simple matter. However, the opposite is true - there is a great risk of data loss and a number of entities that can cause unexpected negative phenomena in these systems, disrupt security, threaten the stability and functioning of the system.[12]

---

[7] J. Šušol, *Elektronická komunikácia vo vede* (Bratislava: Centrum VTI SR, 2003).

[8] Roman Rak, P. Kolitschová, *Bezpečnost a bezpečí – základní pojmy a jejich vnímání*. (Bratislava: Akadémia Policajného zboru v Bratislave, 2019), 28-40.

[9] Roman Rak, D. Kopencová, *Bezpečnostní hrozby, vlastnosti a fáze.* (Bratislava: Akadémia Policajného zboru v Bratislave, 2019), 72-85.

[10] Vincent Holubiczky, *Vzdelaný policajt, garant bezpečnosti In: Polícia ako garant bezpečnosti* (Bratislava: Akadémia Policajného zboru v Braislave, 2018), 105-113.

[11] Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020, príloha 1, page 22

[12] L. Šimák, *Terminologický slovník krízového riadenia: aktualizované vydanie.* (Žilina : Žilinská univerzita v Žiline, 2005).

II. Method

The target group of our research consisted mainly of members of the Police Force of the Slovak Republic and civil servants who use any computing technology in their work, such as a personal computer, laptop, mobile phone or other devices. In addition to this primary group, the questionnaire was distributed for the purpose of comparing the results to other groups, namely employees in the private sector in the field of information technology and full-time students of the Police Academy in Bratislava. The questionnaire was created as an online form. The link to this form was purposefully sent to all senior officers of the Police Force at the level of the Presidium of the Police Force, all regions and districts of the Slovak Republic, and other groups of respondents from the private sector were also addressed. In the case of an online questionnaire, it is very difficult, even impossible, to determine the percentage of completed and returned questionnaires, since the exact number of people who got to the questionnaire and decided not to fill it out is not known. At this point, however, we can say that the link was delivered to more than 2,000 people and the total number of completed questionnaires is 214. This means approximately 10%, while this value may seem low, but in our opinion, it is sufficient for a quantitative and qualitative evaluation of the research.[13]

The main goal of our research was to summarize and analyse knowledge about the state of security of telecommunication and information technologies, used in the activities of the Police Force, by analysing the background of their use (software), technical equipment (hardware) and compliance with relevant legal regulations and internal acts by the operating personnel. In this way, we were able to map the current state of their compliance by the relevant authorities, identify problem areas of security with an emphasis on possible threats and vulnerabilities.

We present an evaluation of the research questions, by answering which we get an insight into the security perception of the research sample and valuable information about their dangerous habits that can lead to security incidents. It is important to remember that the aim of this scientific study is to provide partial research results, therefore we will not devote ourselves to the evaluation of individual questions from the questionnaire, but focus exclusively on the evaluation of selected research questions. It is possible to refer to the results from specific questions of the questionnaire, but these data[14] will always be clearly processed in tables and suitably graphically represented.

III. Research and results

Here we present the research questions that we will try to answer in the following lines and analyse the results. When determining the research questions, we were based on the scientific problem and also on the determined main goal of the research and sub-goals. With the help of these questions we will try to reveal some deeper connections. We set the following research questions:

- Research question no. 1: How does training affect compliance with internal rules?
- Research question no. 2: What are the habits of users who use work equipment for private purposes?
- Research question no. 3: What are the differences in the views on training and support of those who have already completed such training and those who have not?

[13] Vincent Holubiczky, *Prítomnosť hrozieb a zraniteľností pri využívaní informačných technológií.* In: Policajná teória a prax ((Bratislava: Akadémia Policajného zboru v Bratislave, 2020), 5-19.

[14] All data are available upon request from the author of this article.

Some research questions cannot be evaluated simply using only one question from the questionnaire. It is often necessary to use the entire section of questions, or a combination of different sections, in order to clearly clarify the connections. The ideal helper in this case is the use of contingency tables indicating the frequency of responses.

A How does training affect compliance with internal rules?

In this issue, we will address the possibilities of encouraging users to comply with the regulations. We want to find out what effect participation in training has on this. We used two questions from the question section of the "training and support" questionnaire and summarized the results in the table below. It shows the response scales, where 0 means a strong rejection of the statement (definitely not) and the number 5 indicates the strong agreement of the respondent. Such a scale is also used in the evaluation of the remaining questions.
It is clear from the total frequencies that the majority of respondents comply with the regulations.

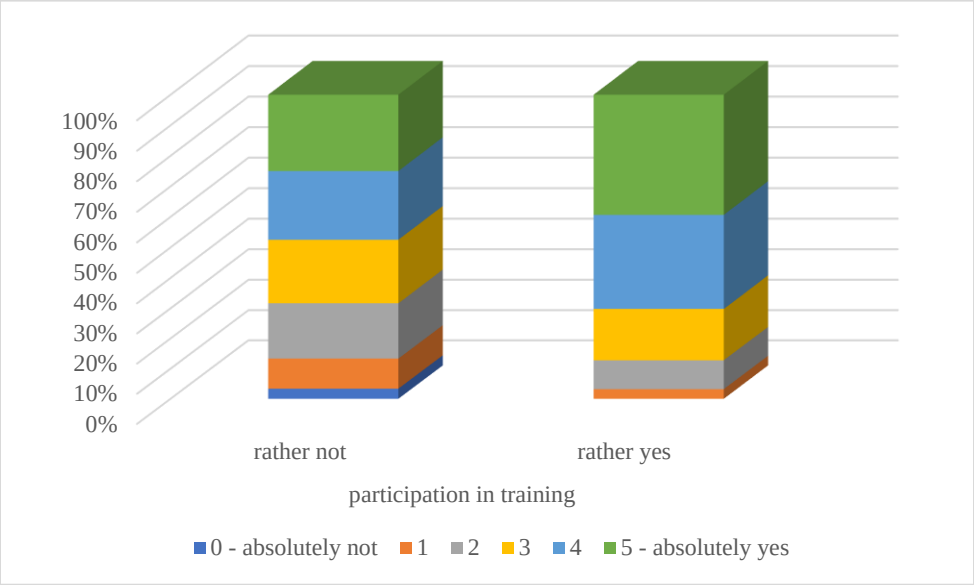
Table 1: The impact of training on compliance with internal regulations[15]

Contingency table for RQ1		Training and support (compliance)						
		0	1	2	3	4	5	Σ
Training and support (participation in training)	0	1	8	9	13	12	16	59
	1	2	2	4	4	12	7	31
	2	1	2	9	8	3	7	30
	3	0	2	3	3	5	7	20
	4	0	0	3	3	12	4	22
	5	0	1	3	10	12	26	52
	Σ	4	15	31	41	56	67	214

We can see the status regarding "participation in information security training" in the graph below. We divided the respondents into two groups. In the first column, there is a group that gave rather negative answers to participation in trainings, the second column of the graph indicates the other respondents. Subsequently, the colour scale indicates their attitude towards compliance with regulations. We can see, not too big, but a noticeable difference, which indicates a positive effect of the training. Only approximately 13% of trained respondents stated that they rather do not comply with the regulations, while on the side of untrained or less trained respondents, this value is as low as 32%.

[15] Source: Compiled by the author.

Figure 1: The impact of training on compliance with internal regulations[16]



We believe that training is an effective tool in the fight against the occurrence of security incidents. We clearly perceive their added value also in terms of information and security awareness of users.

B What are the habits of users who use work equipment for private purposes?

This research question examines the case where users use work equipment and systems for private purposes. We will specifically focus on the security habits of these users, as irresponsible behavior could endanger the integrity, confidentiality and availability of technologies intended primarily and exclusively for work.

Table 2: Habits of users using work computers for private purposes

Contingency table for RQ2		User habits						
		0	1	2	3	4	5	Σ
Purpose (work computer for private purposes)	advertisement	35	12	3	2	1	0	53
	opening	33	8	3	4	4	1	53
	USB	2	4	4	6	15	22	53
	antivirus	3	2	1	1	1	45	53
	Σ	73	26	11	13	21	68	212

[16] Source: Compiled by the author.

Table 3: Habits of users using work email for private purposes

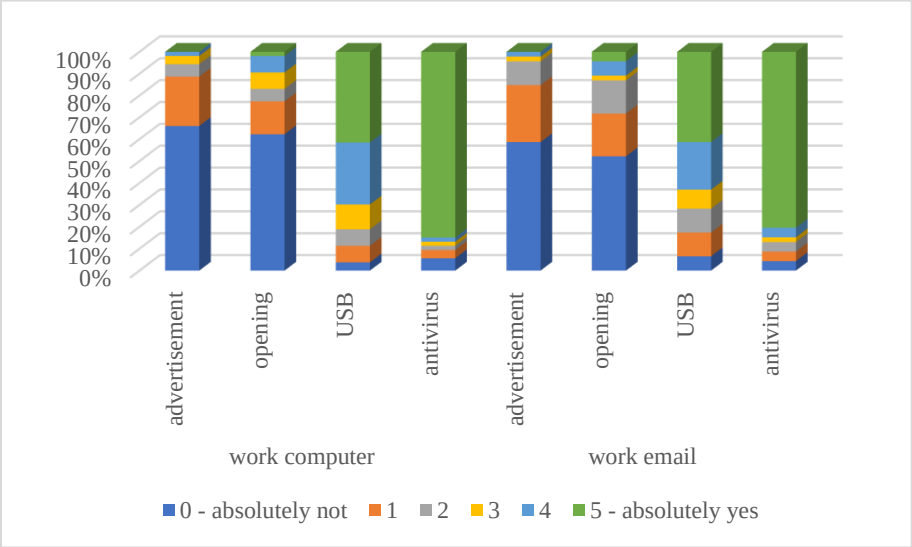
Contingency table for RQ2		User habits						
		0	1	2	3	4	5	Σ
Purpose (work email for private purposes)	advertisement	35	12	3	2	1	0	53
	opening	33	8	3	4	4	1	53
	USB	2	4	4	6	15	22	53
	antivirus	3	2	1	1	1	45	53
	Σ	73	26	11	13	21	68	212

We filtered the range of respondents based on the answers to the items "work computer" and "work email" from the section of questions regarding the purpose of using technology. We take into account only those who confirmed in their answer that they also use work devices for private purposes. Subsequently, we found out the frequency of their answers to questions from the "Habits" section, specifically regarding "advertising offers in e-mail", "opening messages from unknown senders", "using USB to transfer data between computers" and "presence of an antivirus program". The data is shown in the tables above.

We converted the values into percentage indicators by row and created the graph below that clearly presents the results. In the case of advertisements and opening messages from unknown senders, our expectations were fulfilled, as the individuals of the sample group, in both cases, showed a decisive, negative opinion towards them at the level of up to 90%. Even in the case of the use of antivirus applications, the answers of the respondents are at an excellent level, the presence of such software was confirmed by approximately 86% to 89% of them. However, the positive results turn to worrisome when using USB to transfer data between computers. Uncontrolled use of transmission media brings with it a high probability of security incidents. Despite this, up to ¾ of the respondents of the sample group indicated that they use them rather than not.

Based on the above, the answer to the research question can be that, users who use work computers and for private purposes mostly have good habits when working with technologies. They thus mitigate the risk of the influence of threats and vulnerabilities. Of course, with this statement we in no way approve and do not support the elementary fact that they use work equipment for private purposes at all. We hold this opinion especially in the case of using physical transmission media.

Figure 2: Habits of users using work technologies for private purposes



C *What are the differences in the views on training and support of those who have already completed such training and those who have not?*

With the last research question, we want to find out what is the difference in the perception of training by those who have already completed training and those who have never completed training. We divided the respondents into these two groups based on their answers to the question "Have you ever completed information security training?". In the tables, we have named the groups "did not participate", where answers 0 to 2 from the scale are included, and "participated" with values 3 to 5. Subsequently, in the tables below, we present the frequency of responses of these groups to the questions from the "training and support" section. Specifically, regarding the "positive effect of training", "the need to improve qualification", "own feeling of the need to undergo training" and "sufficiency of training offers".

Table 4: Positive effect of training according to participation in training

Contingency table for RQ3		positive effect of training						
		0	1	2	3	4	5	Σ
training and support	did not participate	19	14	27	18	15	27	120
	participated	1	2	12	18	23	38	94
	Σ	20	16	39	36	38	65	214

Table 5: The need to improve qualification according to participation in training

Contingency table for RQ3		the need to improve qualification						
		0	1	2	3	4	5	Σ
training and support	did not participate	3	6	15	24	22	50	120
	participated	0	0	4	15	23	52	94
	Σ	3	6	19	39	45	102	214

Table 6: Own feeling of the need to undergo training according to participation in training

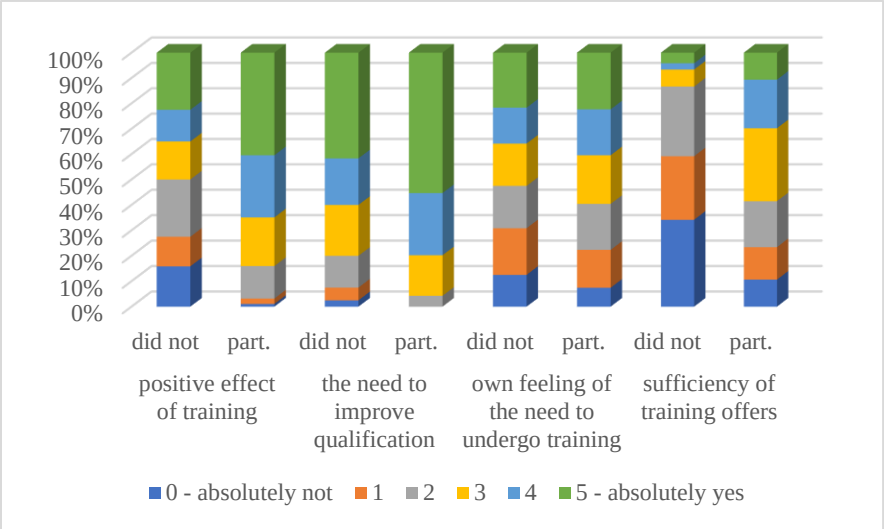
Contingency table for RQ3		own feeling of the need to undergo training						
		0	1	2	3	4	5	Σ
training and support	did not participate	15	22	20	20	17	26	120
	participated	7	14	17	18	17	21	94
	Σ	22	36	37	38	34	47	214

Table 7: Sufficiency of training offers according to participation in training

Contingency table for RQ3		sufficiency of training offers						
		0	1	2	3	4	5	Σ
training and support	did not participate	19	14	27	18	15	27	120
	participated	1	2	12	18	23	38	94
	Σ	20	16	39	36	38	65	214

The results stand out better in the chart below. First of all, we can examine the effect of participation in the training on the perception of its positive effect. If we group the answers to "agree" and "disagree", we find that they are divided exactly in half in the case of "non-participants", while "participants" recognize a positive contribution in up to 84% of cases. The other two columns of the graph show the opinions on the need to improve qualifications. Even if in this case even "non-participants" have a favorable opinion at the level of 80%, their trained colleagues clearly recommend increasing the qualification with a 95% favorable opinion.
In the next question, we asked about the subjective feeling of the respondent's own need to undergo training regarding the security of information systems. The answers of both groups are surprisingly at about the same level and say that they would need such training. In the last assessed question, we find the biggest difference between the answers of individual groups.

Figure 3: The impact of participation in training



More than 86% of respondents without training claim that there is an insufficient amount of them on offer, while the second group holds such an opinion at the level of 41%. Even in this case, we cannot say that such an opinion is acceptable.

From the above statistical data, in our opinion, it is clear that training has a positive impact on the perception of security as a complex system. Awareness is an important key to security and is an effective weapon against the indifference and daily routine of users of information and telecommunication systems.

IV. Results and discussion

Our task was to determine the degree of compliance with internal and legal regulations on security by users of telecommunications and information systems. According to the answers of the respondents, whether they comply with regulations regarding information security, we could accept a very positive conclusion, since up to 76% of them answered it rather positively. The same applies to knowledge of internal regulations. In connection with this, we also pointed out the positive impact of training in this area, as awareness encourages compliance with basic security measures. Based on the above-mentioned findings, we can conclude that, according to the respondents, compliance with internal regulations is at a high level. At the same time, we also emphasize the answers from the habits section, where we find certain shortcomings and claim that it is necessary to direct the users' attention to these items even more.

Therefore, we recommend providing better and more direct access to all information, recommendations, internal regulations, laws and international legal acts on information security in one place, thus creating a space with a comprehensive overview at all levels. Since these documents are designed by experts and are processed at a high professional level, it is assumed that not every user will understand them and then apply them at the required level. Therefore, we suggest adapting the most important sections to the users' knowledge. Subsequently, it is necessary to present direct and simple facts and instructions to them in an appropriate way. A good solution could be various visual aids, simple infographics or short and concise manuals for safe behavior in the workplace.

One of the most important goals of our work is to examine the impact of training on security. It should be noted that less than 45% of the respondents expressed a favorable opinion on completing information security training. This is, in our opinion, a low level of participation. Despite the small participation of the respondents in the training, a high percentage of them recognize the positive effects of the training and its necessity. It is a certain paradox that can be explained by opinions on the training offer. More than 2/3 of the research participants claim that the number of training offers is insufficient. We defend the opinion that awareness is the key solution in the fight against cybercrime and the occurrence of security incidents.

We can add that our recommendation for this topic is its maximum rate of promotion of information at all levels. Information serves as a preventive measure, and we believe that it is more worthwhile to invest in prevention and prevent the consequences. It is necessary to prepare and ensure an adequate amount of training, while it is also desirable to inform users about these possibilities. However, as a first step, we recommend training and securing high-quality trainers, while considering the possible contribution of the best practices and experience of lecturers from the private sector as well.

V. Conclusion

We assumed that through our research we would find certain gaps in the security system of the Police Force, especially in the area of the attitude of the personnel. On a certain level, our expectations in this regard have been fulfilled. But in no case do we want and cannot critically evaluate the work and efforts of the workers responsible for the security of the telecommunications and information systems of the Police Force. We emphasize that after personal consultations with competent people, we perceive this issue even more sensitively and recognize its complexity. It is not possible to find a general solution to some identified shortcomings, and even security managers in the highest positions cannot influence a person's free will. However, we want to point out that long-lasting positive results can be achieved with more frequent and regular training in the field of information security.

VI. References

FELCAN, M. a kol. 2019. *Moderné technológie v páchaní, odhaľovaní, dokumentovaní, dokazovaní a prevencii trestnej činnosti pri zabezpečení verejného poriadku, bezpečnosti a plynulosti cestnej dopravy: Aspekty technické, kriminalistické, kriminologické, penologické, právne, verejno-správne, sociálne, psychologické a bezpečnostné.* VVÚ VÝSK. 245. Akadémia Policajného zboru v Bratislave.

HOLUBICZKY, V. 2020. Frekvencia využívania moderných technológií Policajným zborom. In: *Moderné technológie v páchaní, odhaľovaní, dokumentovaní, dokazovaní a prevencii trestnej činnosti.* Bratislava: Akadémia Policajného zboru v Bratislave. s. 163-171. ISBN 978-80-8054-856-8.

HOLUBICZKY, V. 2020. Moderné technológie a účel ich využívania. In: *Projustice - vedecko-odborný recenzovaný časopis pre právo, spravodlivosť a bezpečnostné vedy.* Roč. 9 (2020). ISSN 1339-1038.

HOLUBICZKY, V. 2020. Prítomnosť hrozieb a zraniteľností pri využívaní informačných technológií. In: *Policajná teória a prax*. Bratislava: Akadémia Policajného zboru v Bratislave. Roč. XXVIII., č. 2, s. 5-19. ISSN 1335-1370.

KOPENCOVÁ, D., RAK, R. 2019. *Risk Analysis and Threats in Security Sciences*. In: Európska veda, vedecký časopis 3/2019. Podhájska: Európsky inštitút ďalšieho vzdelávania. S. 109-115. ISSN: 2585-7738.

RAK, R., KOLITSCHOVÁ, P. 2019. *Bezpečnost a bezpečí – základní pojmy a jejich vnímání.* In: Zborník z 14. medzinárodného sympózia konaného dňa 14. 3. 2019 v rámci medzinárodného veľtrhu SECURITY BRATISLAVA 2019. Bratislava: Akadémia Policajného zboru v Bratislave. s. 28 – 40. ISBN 978-80-8054-795-0.

RAK, R., KOPENCOVÁ, D. 2019. *Bezpečnostní hrozby, vlastnosti a fáze*. In: Zborník z 14. medzinárodného sympózia konaného dňa 14. 3. 2019 v rámci medzinárodného veľtrhu SECURITY BRATISLAVA 2019. Bratislava: Akadémia Policajného zboru v Bratislave. s. 72 – 85. ISBN 978-80-8054-795-0.