Information security risk assessment using the AHP method

J Zaburko and J Szulżyk-Cieplak

Lublin University of Technology, Faculty of Fundamentals of Technology, Nadbystrzycka Str. 38, 20-618 Lublin, Poland
jzaburko@gmail.com

Abstract. This paper is concerned with the issues of cybersecurity and it presents AHP multi-criteria analysis methodology applied for assessing the level of real threats arising from cyberspace that affect the information security. Based on the results of surveys conducted among employees of a selected state institution, we carried out an analysis of awareness of the dangers of cyberspace and ways employees respond to incidents in systems. Taking into account the research results, an appropriate mechanism for the provision of an adequate level of information security was proposed.

1. Introduction

The term security appears in numerous various contexts and is defined differently depending on the field of knowledge or the area of analysis. With the development of civilisation, the term has systematically expanded to include previously unknown challenges and threats, as well as new means and ways to eliminate them [1]. The modern broad understanding of security results from the equally broad understanding of its threats, which goes far beyond the classic military domain. In the 21st century, the humanity has faced threats of a completely new nature as a result of intensive civilisation and technological progress. The development and use of the achievements of science and technology has brought substantial benefits in everyday life, however, numerous dangers entailed. Natural resources are being increasingly exploited, and the natural environment is undergoing gradual degradation, which is particularly evident in relation to air quality, water resources and soil [2-5]. Industry and transport are the key sources of pollution, which has an adverse effect on the health and life of living organisms, is the cause of negative phenomena, both global and local, which in turn requires the use of comprehensive preventive measures and the use of sustainable and the most environmentally sound methods of waste management [6,7].

One of the key features of modern civilisation is the fact that the importance of information is continuously rising. A particularly relevant consequence of this distinction is systematic highlighting the role of information security. In the world dominated by electronics, almost every sphere of life is becoming more and more dependent on Information and Communication Technologies (ICT). ICTs come into an infrastructure which comprises cyberspace, containing data and key systems in many fields. Growing number of computer system security breaches and the safety of users of services offered by modern information and communication technologies means that maintaining security in cyberspace is currently one of the most critical problems at a national and international level. Threats to cyberspace security are becoming more and more advanced, and the scale of incidents is increasing every day. The problem of cybercrime related to illegal activities in cyberspace is also growing, including malware scams aimed at massive attacks on electronic banking accounts or identity theft [8, 9].
Cyberterrorism, which is a new form of crime in the virtual world, has become one of the greatest dangers. The reasons for the emergence of the phenomenon of cyberterrorism can be both political goals or purely for a profit.

Politically motivated cyberterrorism is inspired by the threat of destroying network infrastructure and intimidation or extortion of the government of a given country and citizens by far-reaching destabilising information activities in cyberspace (hacktivism) and physical attacks on ICT systems in order to obtain confidential data [10]. Cyberterrorists use virtual space as a tool for serving propaganda, spreading disinformation and recruiting by: hacking computers (hacking) and IT systems (cracking) to achieve material benefits accessing servers bypassing security (backdoor), eavesdropping on information transmitted between computers and intercepting passwords and logins (sniffing), impersonating another computer (IP spoofing), sending viruses and computer worms (malware), phishing confidential information (phishing) [11].

The typical targets of personalised attacks are:

- military systems storing information about the location of satellites, the location of military bases and long-range weapons as well as the communication systems used by the army of a given country;
- systems in institutions storing information important for the company's operations, such as information about reservations, clients, employed technologies, in which case the main perpetrators are most often employees or former employees who cooperate with competitors or take revenge for poor remuneration;
- systems included in the critical state infrastructure, i.e. systems of: state administration, armed forces and institutions dealing with national defence, energy, telecommunication, transport, services intended for emergency that store information important for national security [12].

Cybercrime is also a crime already known in the real world and is found in newer and newer forms. Identity theft, one of the most common crimes, consists in the deliberate use of another person's personal data, address of residence, PESEL number, most often to achieve financial benefit, which may be performed by setting up fake profiles on social networks, extorting bank loans through websites, using the personal data of another person against their will or using credit cards without its owner's consent [13].

Another example of cybercrime is computer fraud involving extortion of money and other tangible goods by entering into a binding purchase and sale agreement on the Internet, receiving the agreed amount and not sending the goods to the buyer. This phenomenon has been long known but it has intensified in recent years on a large scale.

When analysing the activities of cybercriminals, it may be noticed that they use manipulation techniques based on displaying fictitious goods on well-known sales platforms at prices substantially lower than those in stationary stores. In order for the transaction to be concluded, the buyer must pay the full amount for the ordered goods as well as for postal or courier services to the account indicated in the private message from the seller. The potential victim pays money to the account, the purchased goods never reach the buyer and no attempts to contact the seller bring any results.

Earning money has become a guiding principle for malware writers. Cybercriminals have focused their attention on the possibilities of encrypting data on computers that have received their viruses. In 2013, a virus called CryptoLocker appeared and ushered in the "ransomware" era. It was designed to block available user data and prevent access to the computer through encryption. Data recovery was only possible after making prompt payment of $300, which cybercriminals demanded by displaying information on the computer screen. A method called "asymmetric cryptography" was used to encrypt files [14]. This is a type of cryptography that uses sets of two related keys with a length of 330-660 characters for encryption, but one of the keys must be publicly made available to the recipient. The other key is private and known only to the creator of the virus so, in order to obtain it, one is required to make a payment to his account within a certain time. After ignoring the message and on the expiry of the time limit, the recovery and decryption of files becomes impossible. Opening a crafted, infected attachment received via e-mail usually caused virus infection of files on the disk. These files were usually orders to
pay overdue invoices, underpayments of invoices from the mobile network operator or information from the delivery company about the inability to deliver a parcel.

In 2017, a more dangerous version of CryptoLocker appeared, known as WanaCrypt0r 2.0, which got into computers constituting the critical infrastructure of the attacked state. Due to a massive attack, the virus caused extensive damage by disabling traffic management systems, the work of hospitals, banks and stock exchanges as well as airports and train stations [15].

Hosting companies that make their disk space available for websites or online stores are also highly vulnerable to cyberattacks by using security breaches of crafted software that can break the security of servers storing sensitive data.

According to the website, niebezpiecznik.pl, on 18 December 2018, there was an unauthorised breach of security of the online store, morele.net, the data from whose customer database was obtained. The stolen database contained about 2 million records, including name, surname, e-mail address, password hash, and phone numbers. Breaking of passwords hashes by using "rainbow tables" or specially designed software turned out to be only a matter of time because after two days it was revealed that a criminal had already broken almost 350 thousand passwords. Customers of the online store were notified of a data leak in accordance with the GDPR Directive of 25 May 2018 and also informed the General Inspector for Personal Data Protection.

Company/Institution information resources protection is, therefore, a significant challenge for cybersecurity specialists. Cybersecurity consists in the implementation and proper management of the technical security of an ICT system [16].

Effective security of processed information according to PN-ISO / IEC 27001 should be ensured by:

- confidentiality - the information is available only to those users who have received appropriate permissions and have appropriate security information and declarations;
- integrity - available information is complete, reliable and has not been changed in any way;
- availability - authorised users have access to information at any time when they need it [17].

On 22 January 2015, the President of the Republic of Poland signed the document "Cybersecurity Doctrine of the Republic of Poland," which set out the strategic directions of actions aimed to provide a high level of cybersecurity of the Republic of Poland in the cyberworld. This document indicates the need for the development of state-controlled ICT systems and technologies while maintaining compliance with technologies offered by NATO. Regular security audits were also recommended.

The document of particular importance for the state's cybersecurity is the Act of 5 July 2018 on the National Cybersecurity System, which contains the provision on the creation of Computer Security Incident Response Teams (CSIRT MON, CSIRT NASK and CSIRT GOV). This is the first legal act of this kind in Poland where public administration and the telecommunications industries have also been included. This document imposes a degree of responsibility for maintaining the efficiency of the national critical infrastructure, established pursuant to earlier acts and legal acts, by government ministries responsible for the structure of the state [18,19].

One of the methods of efficient and secure exchange of information is the introduction of mandatory provisions regarding information processing. This document is called a security policy and is a normative document, constituting a set of regulations, rules and procedures according to which the institution manages information and provides IT resources [20-22]. It includes network infrastructure, hardware and software because they make it possible to process information quickly and securely. Lack of implemented procedures may result in excessive chaos in determining the quality and importance of processed information and affect the risks caused by incidents of legal or disciplinary consequences. It is usually said that the weakest link that constitutes a threat in the security chain, is a man because their careless action may lead to the disclosure of information. This may happen when we are dealing with people who are poorly acquainted with broadly understood computerisation. Therefore, it should be noted that when creating security policy rules, all regulations regarding management, exchange, storage and processing of information should have clearly defined rules to be followed by employees. It has been assumed that the above-mentioned document should be submitted for signature after having read it. Another task is to define the security method of the information processing system. The introduced
security policies specify the rules for creating accounts, user identification, the principle of accountability of people logging into the system, requirements as to the length of passwords, its complexity and period of validity in the system. In order for the system to function properly and safely, the managers of the organisational units, in which the system elements are located, are responsible for maintaining the documentation that includes: a list of system users, a list of workstations, a list of active network devices and physical topology of the network.

The method of entering and outputting data is also important for proper system security. It should be determined whether users ought to have independent access to peripheral devices, such as printers and scanners, external or internal CD drives or flash drives used for recording and archiving data, but which are also the source of potential threats. Contingency plans should also be developed in the event of a power outage or physical IT storage medium damage. The antivirus policy for the system should also be specified.

The updated operating system and antivirus programme protect a workstation against infections originating from the network and which may get into the system while performing work duties. Attention should also be paid to crashes and other abnormal functioning of the system that may indicate an attack or a real security breach.

The organiser of the system is required to develop procedures for effective crisis management. Depending on the type and scope of system operation, you should additionally develop procedures for responding to: information system failure and unavailability of the service, malicious code - reporting an incident to CSRIT GOV, violation of confidentiality and data integrity, and misuse of the service in the system.

Procedures for responding to crisis should include provisions regarding: a correct description of the problem encountered, including its scope, identification of the cause of the incident, planning corrective actions to prevent the reoccurrence of the event and how to document the solution to the problem [21, 23].

Striving to eliminate losses or minimise them is an indispensable component of the proper functioning of the institution. In this aspect, it is necessary to properly manage security and manage risks. In order to ensure the appropriate level of security in an institution, it is necessary to conduct a detailed analysis of the resources at risk, taking into account potential threats. Risk estimation is necessary in the scope of detailed identification of threats to information security and an indication of weaknesses that may occur in a given institution. This approach allows both to identify types of risk based on potential threats and to learn techniques and methods to mitigate them, which will consequently result in the institutions’ management implementing appropriate decisions as part of raising the level of information security in the institution

2. Materials and methods
As part of the study, an analysis of the information security system was carried out in one of the state administration sector institutions in Lublin. Identification of potential threats and estimation of risks of information loss in the institution was performed by means of the method of hierarchical analysis of the AHP problem. In the proposed solution, to determine the weights of individual criteria, the experience and knowledge of employees were used. The respondents in the survey determined the impact of individual threats on the risk of information loss. The used method also made it possible to carry out an analysis of the respondents' reliability, which makes the results more objective and reliable.

2.1. The Analytic Hierarchy Process (AHP)
The hierarchical problem analysis (AHP) method, also known as the Saaty method, is one of the best-known multi-criteria decision support methods in the world [24]. Saaty proposed this method for use in many areas to facilitate optimal choices when a decision-maker has more criteria to evaluate different decision options [25]. The advantages of the AHP method, such as flexibility, transparency and ease of use, objectivity of variant selection, the ability to compare both qualitative and quantitative factors,
determine its high popularity and wide application, both in scientific research and solving decision problems [26], including risk analysis [27-29].

The analysis of the decision problem by the AHP method takes place in two phases. The first phase involves developing a hierarchical representation of the problem (Figure 2.). The main goal (problem description) is at the highest level of the hierarchy. At a lower level, the criteria are defined that have an impact on the solution of the analysed problem, and even lower are the sub-criteria that in turn affect the main criteria. The goal of phase two is to generate grades from a mutual comparison of criteria. The criteria are evaluated by a pairwise comparison of elements at each level of the hierarchical model and related to the element at a higher level. A nine-degree, bipolar scale of the importance criteria is used: 1 - equal significance, 3 - slight advantage, 5 - strong advantage, 7 - very strong advantage, 9 - absolute advantage. The numbers 2, 4, 6, 8 are intermediate values and are used only when necessary. The determined comparisons form a square matrix of pairwise comparisons \( A = \{a_{ij}\}_{1 \leq i,j \leq n} \), where \( a_{ij} \in \{1,2,\ldots,9\} \) for \( 1 \leq i < j \leq n \), and \( n \) is the number of compared pairs of elements (Figure 1.).

In the matrix, \( n(n-1)/2 \) reversible pairwise comparisons are made, for which \( a_{ij} = 1/a_{ji} \). A characteristic feature of this matrix is the diagonal, whose elements have the value of 1 [25].

\[
A = \begin{bmatrix}
1 & a_{12} & \ldots & a_{1n} \\
1/a_{12} & 1 & \ldots & a_{2n} \\
\vdots & \ddots & \ddots & \vdots \\
1/a_{1n} & \ldots & 1/a_{2n} & 1 \\
\end{bmatrix}
\]

**Figure 1.** Comparison matrix [30].

In the next step the pair comparison matrix \( A \) is transformed (normalised) into matrix \( B = [b_{ij}] \), whose individual elements are equal to:

\[
b_{ij} = \frac{a_{ij}}{\sum_{i=1}^{n} a_{ij}} \]  \hspace{1cm} (1)

The weights of the evaluated elements are determined as arithmetic means of rows of the normalised matrix \( B \):

\[
w_i = \frac{1}{n} \sum_{j=1}^{n} b_{ij} \]  \hspace{1cm} (2)

Ratings from experts are not always completely objective; in order to eliminate them the CR inconsistency factor has been introduced:

\[
CR = \frac{CI}{RI} \times 100\% \]  \hspace{1cm} (3)

where: \( CI \) – consistency (consequence) index, \( RI \) – random index

The CR coefficient determines to what extent the mutual comparisons of the validity of the characteristics are inconsistent (inconsequent). It is assumed that to consider the results as consistent, the value of the CR coefficient cannot exceed 0.10 (10%).

The basis for calculating the CR coefficient is the determination of the so-called largest eigenvalues \( \lambda_{\text{max}} \) of matrix \( A \). They are calculated in a simplified way as the sum of the products of the sum of the values of comparisons in each column of matrix \( A \) and the appropriate weighting factor for a given element:

\[
\lambda_{\text{max}} = \sum_{i=1}^{n} \left( \sum_{j=1}^{n} a_{ij} \cdot w_i \right) \]  \hspace{1cm} (4)

The consistency factor \( CI \) is then calculated:
Tables of the RI index were generated by Saaty based on the simulations for 500,000 matrices and their values are presented in Table 1 [31].

2.2. Hierarchical model development
In order to determine the importance of individual information security threats in the analysed institution, a set of assessment criteria and sub-criteria was established. Based on the analysis of the literature on the subject [16,32], three main criteria were identified: human-dependent, technical and random threats. The hierarchy of the criteria for assessing the risk of information loss in the institution is shown in Figure 2.

Figure 2. The hierarchical model of the problem (own work).

2.3. Course of research
By definition, the AHP method is based on the assessments of one decision-maker, or assessments of a brainstorming group. For the purposes of research, it was assumed that for correct comparisons, it is important to have theoretical or practical knowledge in the field of the analysed issues and to assess the weight of criteria, the assessments of experts, i.e. employees of institutions having daily contact with information processing, were used. To this end, a questionnaire was prepared which assessed the individual criteria, comparing them in pairs at each level of the hierarchy, giving importance to one of them according to a given scale. The research used a graphic presentation in the form of a table containing a bipolar verbal scale with a midpoint in a vertical arrangement. A fragment of the questionnaire and the method of responding are presented in Figure 3.
Violation of procedures (VP) | (VP) is definitely more important than (UO)
---|---
(VP) is a lot more important than (UO)
(VP) is much more important than (UO)
(VP) is not much more important than (UO)
Both factors are equally important
(UO) is not much more important than (VP)
(UO) is much more important than (VP)
(UO) is a lot more important than (VP)
(UO) is definitely more important than (VP)

Unauthorised operation (UO)

| Employee 1 | Employee 2 | Employee 3 | Employee 4 | Employee 5 | Employee 6 | Employee 7 | Employee 8 |
|---|---|---|---|---|---|---|---|
| Human Dependent | 0.55 | 0.39 | 0.59 | 0.63 | 0.33 | 0.46 | 0.29 | 0.22 |
| Technical | 0.37 | 0.50 | 0.32 | 0.32 | 0.53 | 0.48 | 0.50 | 0.67 |
| Random | 0.08 | 0.11 | 0.09 | 0.05 | 0.14 | 0.06 | 0.21 | 0.11 |
| CR index | **0.092** | **0.071** | **0.085** | 0.121 | 0.173 | **0.062** | 0.182 | 0.224 |

3. Results and discussion
The study involved 8 employees who completed specialist training in information security, including 2 people who were appointed as Personal Data Protection Inspectors. Bearing in mind the course of conduct presented in the AHP method, weights of individual criteria (main criteria and sub-criteria) were calculated in relation to each of the respondents. Sample calculation results are presented in Table 2. and Table 3.

Table 2. Weight values for the main criteria and CR inconsistency coefficients for each respondent (own work).

| Employee 1 | Employee 2 | Employee 3 | Employee 4 | Employee 5 | Employee 6 | Employee 7 | Employee 8 |
|---|---|---|---|---|---|---|---|
| Human Dependent | 0.55 | 0.39 | 0.59 | 0.63 | 0.33 | 0.46 | 0.29 | 0.22 |
| Technical | 0.37 | 0.50 | 0.32 | 0.32 | 0.53 | 0.48 | 0.50 | 0.67 |
| Random | 0.08 | 0.11 | 0.09 | 0.05 | 0.14 | 0.06 | 0.21 | 0.11 |
| CR index | **0.092** | **0.071** | **0.085** | 0.121 | 0.173 | **0.062** | 0.182 | 0.224 |

Table 3. Weight values for the "human-dependent" sub-criterion and CR inconsistency coefficients for each respondent (own work).

| Employee 1 | Employee 2 | Employee 3 | Employee 4 | Employee 5 | Employee 6 | Employee 7 | Employee 8 |
|---|---|---|---|---|---|---|---|
| Violation of procedures | 0.62 | 0.35 | 0.55 | 0.45 | 0.51 | 0.39 | 0.41 | 0.29 |
| Unauthorised Operating | 0.19 | 0.31 | 0.22 | 0.44 | 0.33 | 0.42 | 0.37 | 0.42 |
| Violation of Access | 0.19 | 0.34 | 0.23 | 0.11 | 0.16 | 0.19 | 0.22 | 0.29 |
| CR index | 0.152 | **0.061** | **0.085** | 0.111 | 0.173 | **0.052** | **0.072** | 0.194 |

Using the calculated values of CR inconsistency coefficients, the level of reliability of individual respondents was determined. To assign weights to individual respondents, the AHP method was used, comparing CR indexes with each other and using the assessment scale presented in Table 4. [33]. The calculated weights of individual respondents are summarised in Table 5. Value 0 was assigned to respondents for whom CR > 0.10.
Table 4. The comparative scale of respondents’ reliability [33].

| Points | 1   | 2   | 3   | 4   | 5   | 6   | 7   | 8   | 9   |
|--------|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| The $r$ difference of CR indexes | $r < 0.02$ | $0.02 \leq r < 0.03$ | $0.03 \leq r < 0.04$ | $0.04 \leq r < 0.05$ | $0.05 \leq r < 0.06$ | $0.06 \leq r < 0.07$ | $0.07 \leq r < 0.08$ | $0.08 \leq r < 0.09$ | $r \geq 0.09$ |

Table 5. Values of weights by individual respondents (own work).

| Main criterion | Employee 1 | Employee 2 | Employee 3 | Employee 4 | Employee 5 | Employee 6 | Employee 7 | Employee 8 |
|----------------|------------|------------|------------|------------|------------|------------|------------|------------|
| Sub-criterion „Human dependent” | 0.301 | 0.187 | 0.205 | 0 | 0 | 0.199 | 0.108 | 0 |
| Sub-criterion „Technical” | 0 | 0.232 | 0.177 | 0 | 0 | 0.252 | 0.339 | 0 |
| Sub-criterion „Random” | 0.379 | 0 | 0 | 0.268 | 0.144 | 0 | 0 | 0.209 |

The total weights of the $i$-th criterion $W_i$ were calculated using the formula [33]:

$$W_i = \sum w_{ij} \cdot w_{rj}$$  \hspace{1cm} (6)

where: $w_{ij}$ - weight of the $i$-th criterion according to the $j$-th respondent, $w_{rj}$ - weight of the $j$-th respondent.

Based on formula 6, weights of the main criteria of information loss risk assessment in the analysed institution were calculated, which allowed estimating the significance of individual groups of information loss threats (Figure 4.).

Figure 4. Significance of individual groups of information loss threats (own work).
Based on the results obtained from the computations, it can be concluded that the risks associated with the loss of information most often occur due to human factors (48.23%). Technical hazards are listed second (42%) and the least impact on the risk of information loss is random events that have reached significance at (9.77%).

Similarly, calculations were made to determine the weights of individual sub-criteria for each of the main criteria. Figure 5 shows the estimated risk of information loss for all sub-criteria adopted.

![Figure 5. Risk of information loss in relation to individual threats (own work).](image)

Thus obtained results served to determine which of the considered threats is the most real and which is the least. The most real human-dependent threat is the violation of the institution's procedures (41.58%), unauthorised operating (34.21%) and violation of access (24.21%). Random threats related to an industrial disaster have the least impact on the analysed risk of information loss. The risk of this phenomenon has been estimated at (8.91%).

4. Conclusion
The study conducted at the public institution enabled us to make a subjective assessment of the awareness of employees of a selected state institution regarding the threats of cyberspace. It should also be emphasised that the ability to measure non-compliance using this calculation procedure is seen as an advantage of the AHP method because it allows checking whether the experts participating in the survey answered the questions presented in a thoughtful and not accidental manner. According to the assessment of experts selected from the examined institution, information is usually lost due to human factors. Failure to comply with the guidelines contained in internal procedures may result in the violation of the information security policy, which clearly defines the rules related to access to data and work with information. Actions that should be taken to help employees understand the importance of cyberspace security include the intensification of training frequency and verification of knowledge obtained through tests conducted during training. Constant cooperation with IT staff and reporting observed irregularities in the operation of Information and Communication Technologies systems allows taking effective measures to prevent information disclosure or data leakage.

From the point of view of information protection, it is also recommended to prohibit the use of wireless technologies that pose a potential threat of being hacked into this network. It is also worth
paying attention to the mobile solutions used in companies. These solutions guarantee the security of transmitted information in the form of encrypted connections, location of a lost or stolen device, information management on the phone from two levels - the user and the employee. Such a solution, although not cheap, as the final recipient of the technology is obliged to accept the offer of only one producer, is effective at the level of information security. It should be remembered, however, that the weakest link will always be a man who, whether consciously or not, can effectively deprive institutions of data and information.

5. References

[1] Fałdowski M 2018 Współczesny wymiar bezpieczeństwa Zeszyty Naukowe SGSP 66(2) 109-22

[2] Bieganowski A, Józefaciuk G, Bandura L, Guz Ł, Łagód G and Franus W 2016 Evaluation of hydrocarbon soil pollution using E-nose Sensors 18(8) 2463

[3] Guz Ł, Łagód G, Jaromin-Gleń K, Guz E and Sobczuk H 2016 Assessment of batch bioreactor odour nuisance using an e-nose Desalination and Water Treatment 57(3) 1327-35

[4] Łagód G, Malicki J, Chomczyńska M and Montusiewicz A 2007 Interpretation of the results of wastewater quality biomonitoring using saprobes Environmental Engineering Science 24(7) 873-80

[5] Ratner B 2018 Environmental security: dimensions and priorities. Scientific and Technical Advisory Panel to the Global Environment Facility Washington DC

[6] Kamavisdar A 2010 Heavy metal pollution and their effects on environmental health Indian Journal of Environmental Protection 30(4) 335-40

[7] Widomski M, Gleń P and Łagód G 2017 Sustainable Landfilling as Final Step of Municipal Waste Management system Problems of sustainable development 12(1) 147-55

[8] Damphousse K and Smith B 1998 The Internet: A Terrorist Medium for the 21st Century,” in Kushner, H. W. (ed.), The Future of Terrorism: Violence in the New Millennium, London: Sage 208–24

[9] Denning D E 2002 Wojna Informacyjna i Bezpieczeństwo Informacji (WNT Warszawa)

[10] Kołodziejczyk R 2017 Nowa odsłona terroryzmu - cyberteroryzm Rocznik Bezpieczeństwa Międzynarodowego 17(2) 147-55

[11] Chen T, Jarvis L and Macdonald S 2014 Cyberterrorism: Understanding, Assessment and Response (Springer New York)

[12] Kowalewski J and Kowalewski M 2014 Cyberteroryzm szczególnym zagrożeniem bezpieczeństwa państwa Telekomunikacja i techniki informacyjne 1-2 24-32

[13] Weijer van de S, Leukfeldt R and Bernasco W 2019 Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking European Journal of Criminology 1(4) 486-508

[14] Wobst R 2002 Kryptologia. Budowa i Łamanie Zabezpieczeń (Wydawnictwo RM Warszawa)

[15] Terlikowski M and Madej M 2009 Bezpieczeństwo Teleinformatyczne Państwa (Polski Instytut Spraw Międzynarodowych Warszawa)

[16] Górny P and Krawiec J 2016 Cyberbezpieczeństwo - podejście systemowe Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej 2(18) 78

[17] Kwiecinska M 2014 Wykorzystywanie mediów dla podmienienia bezpieczeństwa, potrzeby i sposoby realizacji Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej 3(11) 75-86

[18] Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej 2015 (BBN Warszawa)

[19] Krajowe ramy polityki cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 2017 (Ministerstwo Cyfryzacji Warszawa)

[20] PN-ISO/IEC 27001:2007, Technika Informatyczna - Techniki bezpieczeństwa - Systemy Zarządzania Bezpieczeństwem Informacji - Wymagania 2007 (PKN Warszawa)

[21] PN-ISO/IEC 27001:2014 - Technika Informatyczna - Techniki Bezpieczeństwa - Systemy Zarządzania Bezpieczeństwem Informacji - Wymagania 2014 (PKN Warszawa)
[22] PN-EN 50131-1 – Systemy Alarmowe Systemy Sygnalizacji Włamania i Napadu Wymagania systemowe 2009 (PKN Warszawa)

[23] Biernacki B and Kalman L 2018 Systemy i Sieci Teleinformatyczne Sił Zbrojnych RP - Wielorakie Aspekty Bezpieczeństwa Cyberprzestrzeni (Akademia Sztuki Wojennej Warszawa)

[24] Saaty T 1972 An Eigenvalue Allocation Model for Prioritization and Planning University of Pennsylvania 28-31

[25] Saaty T 1980 The Analytic Hierarchy Process: Planning Priority Setting Resource Allocation (New York International Book Company New York)

[26] Saaty T 2008 Decision making with the Analytic Hierarchy Process International Journal of Services Sciences 1(1) 83-98

[27] Janackovic G, Savic S and Stankovic I 2013 Selection and ranking of occupational safety indicators based on fuzzy AHP: A case study in road construction companies South African Journal of Industrial Engineering 24(3) 175-89

[28] Meng M and Enping L 2015 The Application Research of Information Security Risk Assessment Model Based on AHP Method Journal of Advances in Information Technology 6(4) 201-206

[29] Ning X and Dong MZ 2011 The Research of Information Security Risk Assessment Method Based on AHP Advanced Materials Research 187 575-80

[30] Adamus W and Gręda A 2005 Wspomaganie decyzji wielokryterialnych w rozwiązywaniu wybranych problemów organizacyjnych i menedżerskich. Badania Operacyjne i Decyzje 15(2) 10

[31] Alonso J and Lamata M 2005 A Statistical Criterion of Consistency in the Analytic Hierarchy Process (MDAI 2005 Springer-Verlag Berlin Heidelberg)

[32] Whitman M 2003 Enemy at the gates: Threats to information security Communication of the ACM 48(8) 91-96

[33] Łękawa Z 2011 Metoda AHP w ocenie zdolności kredytowej jednostki samorządu terytorialnego Annales Universitatis Maria Curie-Skłodowska 2 237