Method of Assessing the Influence of Personnel Competence on Institutional Information Security

Ihor Pilkevych[a], Oleg Boychenko[a], Nadiia Lobanchykova[b], Tetiana Vakaliuk[b], and Serhiy Semerikov[c,d,e]

[a] *Korolov Zhytomyr Military Institute, 22, Prospect Myru, Zhytomyr, 10004, Ukraine*
[b] *Zhytomyr Polytechnic State University, Chudnivska str., 103, Zhytomyr, 10005, Ukraine*
[c] *Kryvyi Rih State Pedagogical University, 54 Gagarin av., Kryvyi Rih, 50086, Ukraine*
[d] *Kryvyi Rih National University, Vitalii Matusevych str., 27, Kryvyi Rih, 50027, Ukraine*
[e] *Institute of Information Technologies and Learning Tools of the NAES of Ukraine, M. Berlynskoho str., 9, Kyiv, 04060, Ukraine*

Abstract

Modern types of internal threats and methods of counteracting these threats are analyzed. It is established that increasing the competence of the staff of the institution through training (education) is the most effective method of counteracting internal threats to information. A method for assessing the influence of personnel competence on institutional information security is proposed. This method takes into account violator models and information threat models that are designed for a specific institution. The method proposes to assess the competence of the staff of the institution by three components: the level of knowledge, skills, and character traits (personal qualities). It is proposed to assess the level of knowledge based on the results of test tasks of different levels of complexity. Not only the number of correct answers is taken into account, but also the complexity of test tasks. It is proposed to assess the assessment of the level of skills as the ratio of the number of correctly performed practical tasks to the total number of practical tasks. It is assumed that the number of practical tasks, their complexity is determined for each institution by the direction of activity. It is proposed to use a list of character traits for each position to assess the character traits (personal qualities) that a person must have to effectively perform the tasks assigned to him. This list should be developed in each institution. It is proposed to establish a quantitative assessment of the state of information security, defining it as restoring the amount of probability of occurrence of a threat from the relevant employee to the product of the general threat and employees of the institution. An experiment was conducted, the results of which form a particular institution show different values of the level of information security of the institution for different values of the competence of the staff of the institution. It is shown that with the increase of the level of competence of the staff of the institution the state of information security in the institution increases.

Keywords

Assessment of the level of knowledge, competence, information threats, a model of the internal violator, model threats.

1. Introduction

The development of information technology provides society with a great variety of electronic services. However, at the same time, there are threats to confidentiality, integrity, and availability of

IntelITSIS'2021: 2nd International Workshop on Intelligent Information Technologies and Systems of Information Security, March 24–26, 2021, Khmelnytskyi, Ukraine
EMAIL: igor.pilkevich@meta.ua (I. Pilkevych); bos_2006@ukr.net (O. Boychenko); lobanchikovanadia@gmail.com (N. Lobanchykova); tetianavakaliuk@gmail.com (T. Vakaliuk); semerikov@gmail.com (S. Semerikov)
ORCID: 0000-0001-5064-3272 (I. Pilkevych); 0000-0003-3048-4184 (O. Boychenko); 0000-0003-4010-0308 (N. Lobanchykova): 0000-0001-6825-4697 (T. Vakaliuk); 0000-0003-0789-0272 (S. Semerikov)

information. Therefore, in recent years, more attention has been paid to the protection of information in institutions (enterprises): measures are organized and carried out to prevent the loss, modification, unauthorized access (acquaintance), leakage, recovery of damaged or lost information. Information security services are also being set up to ensure constant monitoring of the technical condition and software of the information security system, information security, and actions of the institution's personnel who are users of the institution's information and telecommunication system (ITS).

Modern information security systems can effectively counter threats from the outside through the use of antivirus, firewalls, and other specialized software (SS). However, the disadvantage of such an SS is the lack of effective solutions to counter internal threats. To protect against internal threats, a separate SS is used, the effective use of which requires the staff of the Information Security Service (ISS) to have the appropriate knowledge and skills to operate this type of software.

The results of the analysis of internal threats for 2019, presented in the annual report of Cybersecurity Insiders and Gurucul [1], show that the number of insider attacks in 12 months increased by 68% and only 48% of surveyed institutions are confident in protecting their information from internal threats. The same report states that to counter internal threats, 49% of institutions have chosen the tactics of training (education) of ITS users of the institution and the person.

Therefore, this study is aimed at solving the scientific and practical problem of assessing the impact of staff competence on the state of information security of the institution.

2. Related works

The human factor in ensuring the information security of institutions (enterprises) is often ignored. Thus, the report [2] provides an analysis of information security (IS) risks that arise due to irresponsibility and low competence of the staff of the institution (enterprise). The author emphasizes the relevance of the culture of information security, which consists of the observance of the rules of "digital hygiene" by the staff of the institution.

In the article [3], the authors investigated cyber hygiene and its role in information security. They found that those individuals with good cyber hygiene follow best practices for security and protect their personal information.

The authors in the scientific work [4] emphasized the need to consider the level of professional training of employees responsible for IS, as a separate factor influencing the state of IS institution. It was also suggested to improve the selection of employees at the hiring stage and to take appropriate measures to improve their professional level (competence) to prevent or minimize unintentional mistakes.

In the report [5] the author provides a list of methods for detecting insider attacks. The results of the analysis of these methods allow us to conclude that to successfully counter insider attacks, ISS staff must have a high level of professional training and constantly improve it through training in thematic courses and training on IS.

In [6], the authors examined the threat management programs used by firms that provide financial services. These programs began to take into account threats from trusted employees, contractors, and business partners. One such program is the Guide to Insider Threats [7]. This threat management program provides a tool for assessing the trust of employees and the organization of information security in the enterprise.

Several approaches are used to counter insider attacks. The authors [8] suggest using models that are using linguistic analysis to determine an employee's risk level of computer-mediated communication, particularly emails. In [9], the authors suggest using advanced deep learning techniques, which provide a new paradigm to learn end-to-end models from complex data.

Another area of countering insider is information security management. According to research [10], the authors found that numerous activities of management, particularly development and execution of information security policy, awareness, compliance training, development of effective enterprise information architecture, IT infrastructure management, business, and IT alignment, and human resources management, had a significant impact on the quality of management of information security.

Institutional IS depends on the competence of the institution's staff. In the article [11] the authors proposed Competency Model and Instrument for Competency Measurement.

The report [12] presents the views of the international community on the prospects for the development of education for cybersecurity professionals. The authors propose to consider the discipline of cybersecurity as multidisciplinary and provide ways to improve the training of cybersecurity professionals. A modern view on the construction of a model of competence of a specialist in the field of information technology is given in [13]. The authors propose to use the following components of the competency model: personal characteristics, the ability of a person to perform certain functions, a set of types of behavior, and social roles. The authors in the article [14] introduce the concept of mathematical competence of future IS specialists. Mathematical competence is the acquisition of mathematical knowledge and its implementation in the form of professionally significant skills and abilities. The competence approach with the separation of general and special competencies is considered in scientific research [15-18]. These studies propose two approaches to describe competencies: generalization - providing a list of competencies with comments on each component; structural and functional - a description of the stages, functions of activities with access to the generalization of information. In [19-20] techniques concerning cyberattacks detection presented for information security assessment are presented.

Thus, a large number of scientific papers are devoted to the study of competencies, but the issue of the impact of staff competence on the information security of the institution (organization) is not sufficiently studied. The purpose of the article is to develop a method for assessing the impact of staff competence on the information security of the institution using a structural and functional approach to the description of staff competencies.

3. Method of assessing the influence of personnel competence on institutional information security

Competence in this scientific and practical research should be understood as a set of knowledge and skills, as well as personality traits, the use of which allows the individual to solve a specific problem. Assessment of the level of knowledge is based on the methods and techniques of modern Item Response Theory, which provides tools for determining the level of knowledge tested by the results of test tasks, which are evaluated by some continuous value that takes values from [0… 1]. The relationship between the level of knowledge and the performance of test tasks is determined by some nonlinear dependence [21 - 24]. It is the assessment of the level of knowledge is a quantitative indicator of the totality of knowledge and skills of the individual.

In our opinion, (we think that), the competence of the individual functionally depends on the knowledge, skills, and personality traits. If we introduce the coefficients of the importance of knowledge, skills, and personality traits, the competence of the individual will be as follows:

$$Comp = \alpha_1 Sca + \alpha_2 Sk + \alpha_3 Ch \quad (1)$$

where Sca – assessment of the level of knowledge;

Sk – skills assessment;

Ch – assessment of character traits (personal qualities);

$\alpha_1, \alpha_2, \alpha_3$ – coefficients of the importance of assessment of knowledge, skills, and character traits. In this case, the condition must be met: $\alpha_1 + \alpha_2 + \alpha_3 = 1$.

Assessment of the level of knowledge is obtained by testing. To assess the level of knowledge tested by the results of test tasks, a mathematical model was used, which defines the following steps:

1. Calculation of the complexity of the test (complexity of the test). The complexity of the test is characterized by the number of tasks of different levels of complexity and determines the maximum score that can be obtained by the test subject, provided all the correct answers to the test tasks:

$$Ct = \frac{\sum_{i=1}^{m} n_i \cdot tc_i}{m}, \quad (2)$$

where m – the number of levels of difficulty of tasks; n_i – number of tasks i-th level of complexity; $i = 1...m$; tc_i – task complexity, which is calculated by expression:

$$tc_i = \frac{m+1-i}{m}. \quad (3)$$

2. Calculation of the quality of the answer. The quality of the answer is a continuous random variable distributed on the interval [0… 1], which characterizes the completeness of the correct answer:

$$qa_i = \frac{k-i}{k-1}, \quad (4)$$

where k – the number of options for answers to the test task; $i = 1...k$.

3. Calculation of the probability of the correct answer. The probability of the correct answer depends on m – the number of levels of complexity of the tasks, it is determined by this ratio:

$$pca_i = \frac{i}{m} \quad (5)$$

where m – the number of levels of complexity of the tasks; $i = 1...m$.

4. Calculation of the answer level. The level of the answer Al is a continuous random variable distributed on the interval [0… 1], which characterizes the completeness of the correct answer obtained for the problem with the corresponding level of complexity. The level of response does not take into account the probability of the correct answer to the task and the complexity of the task. Then the level of the answer Al is calculated by the following expression:

$$Al_i = qa_{i,l} \cdot tc_{i,j}, \quad (6)$$

where $i = 1...n$; $l = 1...k$; $j = 1...m$; n – number of test tasks.

5. Calculation of the share of correct answers. The share of correct answers Sca is a continuous random variable distributed on the interval [0… 1], which characterizes the level of knowledge based on the quality of answers obtained to tasks of different levels of complexity:

$$Sca = \frac{\sum_{i=1}^{n} Al_i}{n}. \quad (7)$$

Assessment of the level of skills is based on the results of a specially developed set of practical tasks. Assessment of the level of skills is calculated as the number of correctly performed practical tasks to the total number of practical tasks.

Assessment of character traits (personal qualities) is based on the results of special psychological tests. The list of character traits that a person must have to effectively perform the tasks assigned to him, is developed separately for each position. For each position in the institution, the required list of character traits Fch consist x s of elements. The importance of each character trait is determined by the weighting factor β_i. With $\sum_{i=1}^{x} \beta_i = 1$. Then the following ratio should be used to calculate the assessment of personality traits:

$$Ch = \sum_{i=1}^{x} Fch_i \cdot \beta_i. \quad (8)$$

Under the IS of the institution in this study, we will understand the state of protection of information of the institution from many threats of information, which is determined by the model of threats to information of the institution. Dependence of IS on information threats is presented as an expression:

$$IS = \frac{\sum_{i=1}^{b} \sum_{j=1}^{c} z_{i,j}}{b \cdot c}, \quad (9)$$

where $z_{i,j}$ – the probability of occurrence of the i-th threat of information from the set of threats of information Z from the j-th employee of the institution; b – the number of information threats Z, which is determined by the model of information threats of the institution; c – number of employees of the institution.

The probability of occurrence of the i-th threat of information from the set of threats of information from the j-th employee of the institution is influenced by his competence. To find the quantitative value $z_{i,j}$, the method of calculating the probability of realization of information threats from an internal violator was used [25]. This method takes into account the motive of illegal actions by the internal violator and the assessment of his knowledge about the possibility of realizing the threats of information of the institution. When using the method of calculating the probability of realization of information threats from an internal violator in this study, the competence of the internal violator was used instead of assessing his knowledge. According to the method [25] and taking into account the above, the expression for calculating the probability of occurrence of the i-th threat of information from the set of threats to information Z from the j-th employee of the institution:

$$z_{i,j} = M_j + R_{i,j} + Comp_j - M_j \cdot R_{i,j} - M_j \cdot Comp_j - R_{i,j} \cdot Comp_j + M_j \cdot R_{i,j} \cdot Comp_j, \quad (10)$$

where M_j – the probability of the motive of illegal behavior of the employee of the institution; $R_{i,j}$ – the probability of realization of threats by an employee of the institution on the grounds given in the model of the violator.

4. Experiment

Examples are considered to verify the method of assessing the impact of staff competence on the IS of the institution.

Example 1. The institution has a list of positions. The results of the assessment of the level of competence of the staff following the list of positions are shown in table 1.

Table 1

The results of the assessment of the level of competence of the staff of the institution

Employee positions	Knowledge	Skill	Traits	Competence
Security Administrator	0,99	0,99	0,95	0,98
Computer network administrator	0,99	0,99	0,98	0,99
System administrator	0,99	0,99	0,92	0,97
Database administrators	0,75	0,79	0,95	0,83
Head of 1 department	0,4	0,25	0,95	0,53
Workstation operator 1 department	0,5	0,3	0,95	0,58
Head of 2 department	0,4	0,25	0,95	0,53
Workstation operator 2 department	0,5	0,25	0,45	0,40
Electrician	0,1	0,1	0,95	0,38
Communication engineer	0,2	0,2	0,95	0,45
Guardian	0,1	0,1	0,94	0,38
Technician	0,1	0,1	0,5	0,23
Cleaner	0,01	0,01	0,95	0,32

Competence was calculated with the following coefficients of importance:

- knowledge assessment – 0,5;
- skills assessment – 0,4;
- assessment of character traits – 0,1.

The internal intruder model is shown in Table 2. The following notation is introduced for this model:

- r1 – the launch of a fixed set of tasks (programs) that implement pre-provided information processing functions - reading (viewing);
- r2 – creation, and launch of own programs with new functions of information processing (draft documents) - modification, deletion, and copying;
- r3 – creation, and launch of own programs with new functions of information processing (valid documents) - modification, deletion, and copying;
- a1 – place of action of employees of the institution within the controlled area;
- a2 – a place of action of employees of the institution within the regime premises without access to ITS hardware and software;
- a3 – the place of action of the employees of the institution within the regime premises with access to ITS hardware and software;
- s1 – the employee has access to the settings of the data transmission channels;
- s2 – the employee uses standard ITS hardware or software;
- s3 – the employee uses additional ITS hardware or software;
- s4 – the employee uses disguise as a registered ITS user.

Table 2
Model of the internal violator

Employee positions	Level of opportunities			Place of action			Methods and ways of action				Σ	Probability of threats
	r1	r2	r3	a1	a2	a3	s1	s2	s3	s4		
Security Administrator	1	1	1	1	1	1	1	1	1	0	9	0,9
Computer network administrator	1	1	1	1	1	1	1	1	1	0	9	0,9
System administrator	1	1	1	1	0	1	0	1	1	0	7	0,7
Database administrators	1	1	1	1	0	1	0	1	1	0	7	0,7
Head of 1 department	1	1	1	1	0	1	0	1	0	0	6	0,6
Workstation operator 1 department	1	1	0	1	0	1	0	1	0	0	5	0,5
Head of 2 department	1	1	1	1	0	1	0	1	0	0	6	0,6
Workstation operator 2 department	1	1	0	1	0	1	0	1	0	0	5	0,5
Electrician	0	0	0	1	1	0	0	0	0	0	2	0,2
Communication engineer	1	0	0	1	1	1	1	0	1	0	6	0,6
Guardian	0	0	0	1	0	0	0	0	0	0	1	0,1
Technician	0	0	0	1	1	0	1	0	0	0	3	0,3
Cleaner	0	0	0	1	0	0	0	0	0	0	1	0,1

Model threats to the information of the institution are shown in Table 3.

Table 3
Model threats to the information of the institution

Type of information threat	Level of	Place of	Methods and	Σ	Probability

	opportunities			action			ways of action					of threats
	r1	r2	r3	a1	a2	a3	s1	s2	s3	s4		
Unauthorized access (z_1)	1	1	1	1	1	1	0	1	1	1	9	0,9
Uncontrolled acquaintance (z_2)	1	1	1	1	1	1	0	1	0	1	8	0,8
Random modification (z_3)	0	1	1	1	0	1	0	1	0	0	5	0,5
Deliberate modification (z_4)	0	1	1	1	0	1	1	1	1	1	8	0,8
Accidental destruction (z_5)	0	1	1	1	0	1	0	1	0	0	5	0,5
Deliberate destruction (z_6)	0	1	1	1	0	1	1	1	1	1	8	0,8
Unauthorized copying (z_7)	0	1	1	1	0	1	1	1	1	1	8	0,8
Random distribution (z_8)	0	0	1	1	0	1	1	1	0	0	5	0,5
Deliberate distribution (z_9)	0	1	1	1	0	1	1	1	1	1	8	0,8

The probabilities of information threats from the staff of the institution are shown in Table 4.

Table 4

Probabilities of information threats from the staff of the institution

Employee positions	z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9
Security Administrator	0,81	0,72	0,45	0,72	0,45	0,72	0,72	0,45	0,72
Computer network administrator	0,81	0,72	0,45	0,72	0,45	0,72	0,72	0,45	0,72
System administrator	0,63	0,56	0,35	0,56	0,35	0,56	0,56	0,35	0,56
Database administrators	0,63	0,56	0,35	0,56	0,35	0,56	0,56	0,35	0,56
Head of 1 department	0,54	0,48	0,3	0,48	0,3	0,48	0,48	0,3	0,48
Workstation operator 1 department	0,45	0,4	0,25	0,4	0,25	0,4	0,4	0,25	0,4
Head of 2 department	0,54	0,48	0,3	0,48	0,3	0,48	0,48	0,3	0,48
Workstation operator 2 department	0,45	0,4	0,25	0,4	0,25	0,4	0,4	0,25	0,4
Electrician	0,18	0,16	0,1	0,16	0,1	0,16	0,16	0,1	0,16
Communication engineer	0,54	0,48	0,3	0,48	0,3	0,48	0,48	0,3	0,48
Guardian	0,09	0,08	0,05	0,08	0,05	0,08	0,08	0,05	0,08
Technician	0,27	0,24	0,15	0,24	0,15	0,24	0,24	0,15	0,24
Cleaner	0,09	0,08	0,05	0,08	0,05	0,08	0,08	0,05	0,08

The probability of occurrence of a motive for the illegal behavior of an employee of the institution for all staff of the institution is equal to 0.25.

Substituting the data from tables 1-4 to expression (9) we obtain a quantitative value of information security, which is equal to 0.658.

Example 2. The institution has a list of positions. The results of the assessment of the level of competence of the staff by the list of positions are shown in table 5.

Table 5
The results of the assessment of the level of competence of the staff of the institution

Employee positions	Knowledge	Skill	Traits	Competence
Security Administrator	0,25	0,25	0,95	0,32
Computer network administrator	0,25	0,25	0,98	0,32
System administrator	0,25	0,25	0,92	0,32
Database administrators	0,2	0,2	0,95	0,28
Head of 1 department	0,15	0,15	0,95	0,23
Workstation operator 1 department	0,1	0,1	0,95	0,19
Head of 2 department	0,1	0,1	0,95	0,19
Workstation operator 2 department	0,1	0,1	0,45	0,14
Electrician	0,1	0,1	0,95	0,19
Communication engineer	0,2	0,2	0,95	0,28
Guardian	0,1	0,1	0,94	0,18
Technician	0,1	0,1	0,5	0,14
Cleaner	0,01	0,01	0,95	0,10

The model of the internal violator, the model of information threats, the probability of information threats from the staff of the institution, and the probability of the motive of misconduct of the employee of the institution used from example 1. Then obtained a quantitative value of information security, equal to 0.545.

Example 3. The institution has a list of positions. The results of the assessment of the level of competence of the staff by the list of positions are shown in table 6.

Table 6
The results of the assessment of the level of competence of the staff of the institution

Employee positions	Knowledge	Skill	Traits	Competence
Security Administrator	0,9	0,9	0,95	0,91
Computer network administrator	0,9	0,9	0,98	0,91
System administrator	0,9	0,9	0,92	0,90
Database administrators	0,9	0,9	0,95	0,91
Head of 1 department	0,5	0,5	0,95	0,55
Workstation operator 1 department	0,4	0,4	0,95	0,46
Head of 2 department	0,5	0,8	0,95	0,67
Workstation operator 2 department	0,8	0,5	0,45	0,65
Electrician	0,5	0,4	0,95	0,51
Communication engineer	0,6	0,8	0,95	0,72
Guardian	0,1	0,1	0,94	0,18
Technician	0,3	0,5	0,5	0,40
Cleaner	0,01	0,01	0,95	0,10

The model of the internal violator, the model of information threats, the probability of information threats from the staff of the institution, and the probability of the motive of misconduct of the employee of the institution were used from example 1. Then obtained a quantitative value of information security, equal to 0.734.

5. Discussions

The study yielded the following results:

1. Assessment of the level of knowledge of employees of the institution is carried out by testing them. The mathematical model, which is used to calculate the level of knowledge of employees of the

institution, takes into account the complexity of test tasks. This model provides an expression for calculating the complexity of the test in general. The complexity of the test has a direct functional dependence on the sum of the product of the complexity of the tasks and their number. It is also proposed to use a mathematical dependence to assess the quality of the answer, which characterizes the completeness of the answer. The use of a mathematical model for assessing the level of knowledge of employees allows the developer of test tasks to obtain tests of different levels of complexity for different positions of the institution.

2. In each institution to ensure information security, a model of threats to the information of the institution and a model of the violator (internal and external) are developed. The threat can be realized with the appropriate probability. To find the quantitative value of the possibility of realizing the threat of information, the method of calculating the probability of realizing information threats from an internal violator was used. In this study, using the method of calculating the probability of realization of information threats from an internal violator, instead of assessing the knowledge of the internal violator, the competence of employees of the institution was used. To take into account the mutual influence of the probability of occurrence of events (realization of information threat, acquisition of appropriate access rights) to calculate the probability of realization of information threat from the set of information threats from an employee, the theorem on the addition of arbitrary events was applied.

3. The results of the experiment indicate that with the increase in the level of competence of employees of the institution, the state of information security in the institution increases. In example 3, where the competence of employees of the institution is the highest, the quantitative value of information security is equal to 0.734. In example 2, where the competence of employees of the institution is the lowest, the quantitative value of information security is equal to 0.545. In example 1, where the competence of employees of the institution is average, the quantitative value of information security is equal to 0.658. In these examples, only the quantitative values of competence of employees of the institution were changed. The model of the internal violator, the model of information threats, the probability of information threats from the employees of the institution, and the probability of the motive for the illegal behavior of the employee of the institution were the same for all examples. The conducted experiments confirm that the information security of the institution has a nonlinear functional dependence on the competence of the employees of the institution.

6. Conclusions

The method of assessing the influence of personnel competence on institutional information security allows obtaining a quantitative value of information security. The proposed method makes it possible to automate the process of assessing personnel competence through the use of the mathematical apparatus of modern test theory, systems analysis, and probability theory. The practical orientation of the study is to use the developed method in the information security service of the institution to assess the possibility of implementing the appropriate type of threat from the staff of the institution, taking into account the level of personnel competence. The method of assessing the influence of personnel competence on institutional information security allows assessing the information security taking into account the model of the violator, the model of information threats, which are designed for a particular institution.

7. References

[1] 2020 Insider Threat Report. Cybersecurity Insiders, URL: https://www.cybersecurity-insiders.com/wp-content/uploads/2019/11/2020-Insider-Threat-Report-Gurucul.pdf

[2] N. Kuharska, Informacijna bezpeka jak element korporatyvnoji struktury Aktual′ni problemy upravlinnja informacijnoju bezpekoju deržavy: zb. tez nauk. dop. nauk.-prakt. konf. (Kyjiv, 4 kvitnja 2019. Kyjiv : Nac. akad. SBU) 70–73.

[3] A. A. Cain, M. E. Edwards, J. D. Still, An exploratory study of cyber hygiene behaviors and knowledge. Journal of Information Security and Applications. Vol. 42 (2018) 36-45.

[4] S.Honchar, H. Leonenko, Analysis of the factors influencing condition cybersecurity of information system of object of the critical infrastructure. Information Technology and Security.

Vol. 4, Iss. 2 (7) (2016) 262-268.
[5] S. Kovalenko. Insajderska zahroza jak odna z aktualnyx problem kiberbezpeky. Osnovni metody vyjavlennja Aktual′ni problemy kiberbezpeky : zb. tez dop. Vseukrajins′koji nauk. konf. (Kyjiv, 24 žovtnja 2019 Kyjiv : DUT) 28–32.
[6] J. Eggenschwiler, I. Agrafiotis, J. RC Nurse, Insider threat response and recovery strategies in financial services firms. Computer Fraud & Security. Vol. 2016, Iss. 11 (2016) 12-19.
[7] W. F. Gross, Insider Threat. Computer and Information Security Handbook. (2017) 529-536.
[8] Faisal Janjua, Asif Masood, Haider Abbas, Imran Rashid, Handling Insider Threat Through Supervised Machine Learning Technique. Vol. 177 (2020) 64-71.
[9] Shuhan Yuan, Xintao Wu, Deep Learning for Insider Threat Detection: Review, Challenges and Opportunities. Computers & Security (2021) 102221.
[10] Z. A. Soomro, M. H. Shah, J. Ahmed, Information security management needs more holistic approach: A literature review. Vol. 36, Iss. 2 (2016) 215-225.
[11] J. Funke, A. Fischer & D. V. Holt, Competencies for complexity: problem solving in the twenty-first century. In Assessment and teaching of 21st century skills, pp. 41-53. Springer, Cham (2018).
[12] A. Parrish, J. Impagliazzo, R. K. Raj, H. Santos, M. R. Asghar, A. Jøsang, T. Pereira, E. Stavrou, Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018 Companion). Association for Computing Machinery, New York, NY, USA, (2018) 36–54. doi: https://doi.org/10.1145/3293881.3295778.
[13] E. Kashtanova, A. Lobacheva, S. Makushkin, T. Ridho, A Competency Model in the Field of Information Technology. In: Bogoviz A.V., Suglobov A.E., Maloletko A.N., Kaurova O.V., Lobova S.V. (eds) Frontier Information Technology and Systems Research in Cooperative Economics. Studies in Systems, Decision and Control, vol 316. Springer, Cham (2021) https://doi.org/10.1007/978-3-030-57831-2_58.
[14] S. Shevchenko, Yu. Zhdanova, Mathematical competencies of future specialists information security. Suchasniy zahist informatsii. 4 (2016) 90-96.
[15] O. Mandzuk, Qualification requirements to the competence of information analytics-lawyers. Scientific notes of Taurida National V. Vernadsky University. Juridical Sciences. 26(68) (2018) 64-72.
[16] V.Buryachok, I.Parhomey, M.Stepanov, V.Tolubko. Problemni pytannja ta aktual′ni zavdannja pidhotovky faxivciv z kibernetyčnoji bezpeky haluzi znan′ «Informacijni texnolohiji». Suchasniy zahist informatsii. 2(2016) 4-9.
[17] M. Bohlouli, N. Mittas, G. Kakarontzas, T. Theodosiou, L. Angelis, M. Fathi, Competence assessment as an expert system for human resource management: A mathematical approach. Expert Systems with Applications, vol. 70 (2017) 83-102.
[18] V. Belevitin, S. Bogatenkov, V. Rudnev, M. Khasanova, A. Tyunin, Integrated approach to modeling IC Competence in students. International Journal of Engineering & Technology, 7(4) (2018) 60-62.
[19] S. Lysenko, K. Bobrovnikova & O. Savenko, A botnet detection approach based on the clonal selection algorithm. In 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). IEEE (2018) 424-428.
[20] S. Lysenko, K. Bobrovnikova, S. Matiukh, I. Hurman & O. Savenko, Detection of the botnets' low-rate DDoS attacks based on self-similarity. International Journal of Electrical & Computer Engineering, 2020, 10, 2088-8708.
[21] D. Magis, J. R. Barrada, Computerized adaptive testing with R: Recent updates of the package catR. Journal of Statistical Software, 76(1) (2017) 1-19.
[22] G. Ling, Y. Attali, B. Finn, E. A. Stone, Is a Computerized Adaptive Test More Motivating Than a Fixed-Item Test? Applied Psychological Measurement, 41(7) (2017) 495–511.
[23] E. D. Heggestad, D. J. Scheaf, G. C. Banks, M. Monroe Hausfeld, S. Tonidandel, E. B. Williams, Scale Adaptation in Organizational Science Research: A Review and Best-Practice Recommendations. Journal of Management, 45(6) (2019) 2596–2627.
[24] Van der Linden, W. J. (Ed.), Handbook of item response theory, three volume set. CRC Press (2018).
[25] O.Boychenko, R.Ziubina. The method of calculation of probability of realization of threats of information with the limited access from an internal user violator. Information systems and technologies security. 1 (2019) 19–26.