Multisociometrical Readiness Characteristics in Information Security Management

Anastasiya Arkhipova [1]

[1] *Novosibirsk State Technical University, 20 Prospekt K. Marksa, Novosibirsk, 630073, Russia*

Abstract

The article discusses the characteristics of Information security management. Information security management system represents as a part of a general management system in organizations. The main tasks that are solved during the information security management and audit of information objects, information security management are formulated. The article considers information security risks from personnel constitute as a separate group of information security risks of the organization with a specific set of causes and conditions for their implementation. The article describes the hypothesis of multisociometrical readiness characteristics construct in Information Security Management as a specific educational component. Thus component, firstly, is an indicator of the readiness of applicants as the most important factor affecting the formation of the competence of a student at the university, secondly, is an indicator of the readiness of a graduate of the university for professional activities, and thirdly, is an indicator of the professionalism of an information security specialist, which is the resulting component of educational activities.

Keywords

education, information security management, information security, cybersecurity level, readiness indicator, social engineering, cybergaming, education characteristics, multisociometrical readiness characteristics

1. Introduction

Ensuring the high quality of education on the basis of preserving its fundamentality and meeting the current and promising needs of the individual, society and the state is one of the main tasks of Russian educational policy. The current state of the educational process, including in the field of information security, is characterized by the mastery of a competent approach to the training of specialists, which consists in the development of key competencies among students that determine their successful adaptation to professional activity.

Analysis of standards, various methodological documents in the field of information security shows the existence of a formal approach to the assessment of specialists in the field of information security (education, seniority, advanced training). The methods lack indicators of the level of professional fitness, competence of employees, criteria for the level of education in the context of theoretical knowledge and practical skills and skills. The set of the above indicators and evaluation criteria, which together represent the educational component, has a direct impact on the employer's activities. Thus, it is now necessary to develop a multisociometrical educational component (multisociometrical readiness characteristics) based on a certain complex qualitative and quantitative indicator in the form of a specialist readiness indicator. The latter will allow the management of enterprises and organizations to make the right decisions on working with personnel and will contribute to improving the level of

AISMA-2021: International Workshop on Advanced in Information Security Management and Applications, October 1, 2021, Stavropol, Krasnoyarsk, Russia
EMAIL: arhipova_ab@mail.ru (Anastasiya Arkhipova)
ORCID: 0000-0003-0791-8087 (Anastasiya Arkhipova)

training of specialists in information security as the most important organizational and technical task of providing information security of the Russian Federation.

Today, in the framework of employment, applicants are not only required to comply with the professional model of the specialist in the context of professional skills (hard skills), but also a certain complex of psychophysiological characteristics (soft skills). Thus, the optimal combination of soft skills and hard skills presents some model of a graduate of an educational institution to the context of a continuous education model [7]. This article attempts to focus on the field of information security [3, 12]. However, it can be extended to other spectra and interdisciplinary areas of research.

The purpose of this article is to describe the technology of generating the multisociometrical readiness characteristics in information security management.

2. Information security management

Information security management system is a part of general management system in organizations. It is based in the group of business risks approach. Its primary objective is to found, implement, exploit, supervise, maintain and improve information security of organizations. Information security management is a systematic approach for managing sensitive information in order to protect it. Information and security is the something beyond of installing a simple fire wall or tying of a contract with a company in the field of information security. In such an approach, it is important that we balance various security activities with a common strategy in order to provide an optimal protection level.

The main purpose of the information security management is to objectively assess the current state of the information security of the organization, for counteracting possible external and internal threats.

Today, conducting an audit of information security management systems is a necessary and required activity. A number of organizations whose business is closely connected with the use of information technologies, such as banks, oil, gas, energy and telecommunications companies, have recently become more active in conducting audits of information security management systems.

The main tasks that are solved during the information security management and audit of information objects, information security management are:

- analysis of structure, functions, used technologies of automated processing and transfer of information to the information objects, analysis of business processes, regulatory and administrative and some technical documents;
- identification of significant information security threats and ways of their implementation; identification and ranking of existing technological and organizational vulnerabilities at the information objects by the danger level;
- development of models of violators, application of active audit techniques to check the possibility of violators implementation of identified information security threats;
- analysis and assessment of risks associated with threats to the security of information resources;
- assessment of the information security management system for compliance with the requirements of the existing information security standards, and development of recommendations for improving the information security management system;
- assessment of the current level of information objects protection and localization of bottlenecks in the protection system;
- development of proposals and recommendations to introduce new and improve the effectiveness of the existing mechanisms for the provision of information security.

Information security risks from personnel constitute a separate group of information security risks of the organization with a specific set of causes and conditions for their implementation.

A set of risk factors represents a single network with causal relationships. Risk factors of the first and second levels are identified. Second-level risk factors mean relatively small phenomena that an organization can work out separately. The group of risk factors of the first level are phenomena that directly and most strongly affect the possibility of implementing threats to information security from personnel. A special place in the organization's personnel system is occupied by information security specialists. They are directly involved in the creation of the Information security management system, its audit and monitoring.

A review of the literature on the development and exploring information security management systems indicates that such systems depend on the human factor [1-2, 5, 7, 11-16].

In order to optimize the processes of information security audit and applicant diagnostics, there is a need to develop an educational component as a multisociometric characteristic, firstly, an indicator of the readiness of applicants as the most important factor affecting the formation of the competence of a student at the university, secondly, an indicator of the readiness of a graduate of the university for professional activities, and thirdly, an indicator of the professionalism of an information security specialist, which is the resulting component of educational activities [7].

3. Technology of multisociometrical readiness characteristics generation in information security management

The specialist readiness indicator is directly related to the subject area, therefore, the specialist readiness technology is logical to build from these positions. Let's take a look at information security. The effective solution of problems in this area requires highly organized, highly qualified personnel support, ranging from the employment procedure to continuous processes of advanced training, retraining taking into account program and technological, organizational changes in the information security of the open state. Moreover, the procedure of employing a specialist from the position of a readiness indicator involves an analysis of its characteristics, while the working process is accompanied by the effect of accumulative frequencies of the factors included in it, as well as the formation of additional links [7].

Therefore, in order to generate a readiness index, it is necessary to enter a group of cumulative factors for the assessment of soft skills and hard skills, as well as nominal characteristics with branching by categories and types/forms of education.

Within the project supported by Charity Foundation of Potanin in 2021 in FGBOOU WAUGH "Novosibirsk State Technical University" is developed in the scientific purposes the automated system of assessment of an indicator of readiness of experts of the direction 10.03.01 "Information security" and 10.05.03 "Information security of the automated systems". This system is a tool for monitoring and analyzing training results. The impact of gamblers in the implementation of programs for the education of an enlarged group of specialties 10.00.00 "Information Security" [7, 15] is also evaluated.

Implementation of the automated system for the readiness indicator modelling can be one of useful methods. Algorithm or the comprehensive approach to the estimation of specialists readiness, based on the results of the expert questioning, accumulated frequencies (fuzzy model with linguistic and point scales). It consists of next blocks:

To create and operate the above-mentioned system, a generalized algorithm for estimating of the multisociometrical readiness characteristics in Information Security Management is implemented as the result of the following units (fig. 1)

Unit 1 is one of the most complex, since it involves the analysis and formalization of criteria and the selection of readiness indicator indicators. Every indicator contains both quantitative and qualitative indicators. Quantitative indicators include specialty/direction data resulting from the competency model in the section of the blocks of disciplines of the curriculum. Qualitative indicators represent a complex of psychophysiological characteristics within the framework of the given direction. Quantitative criteria for choosing indicators should be valid, effective, systemic and measurable (the quantitative and quality aspect).

The technology for generating the specialist readiness indicator is presented in the form of a multi-level structure and involves a consistent solution at all stages: **stage 1, stage 2, stage 3**.

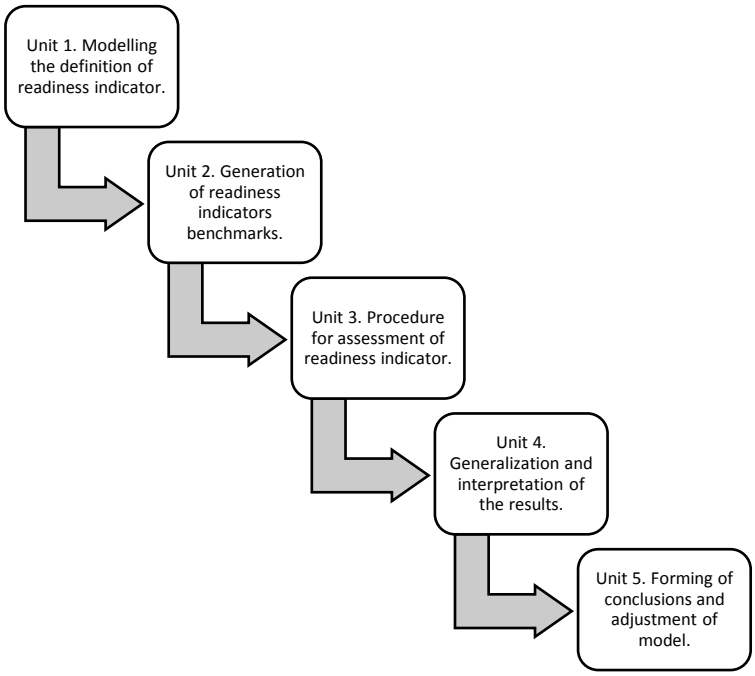

Figure 1: Generalized algorithm for estimating of the multisociometrical readiness characteristics in Information Security Management

Stage 1 is time consuming because it requires the collection and processing of information. By the indicator of readiness of a graduate at this stage is understood: the level of educational achievements of a graduate of an educational institution; an indicator of psychological indicators; the level of interest of the graduate in the field of information security.

1. The level of readiness of a student to study at a university (P_{01}^{1}) is an expression of the following form:

$$P_{01}^{1} = \sum_{j=1}^{n} k_j \cdot \left(\sum_{i=1}^{m_j} \left(D_{X_{ij}} \cdot \alpha \quad \cdot (1-\omega_i) + \omega_i \cdot (1-\alpha \quad) \cdot P_{X_{ij}} \right) \right), \qquad (1)$$

where j – result of curriculum training ($1<j\leq n$, n – disciplines curriculum); k_j - coefficient of significance of disciplines j ($0 < k_j < 1$); $D_{X_{ij}}$- total result X_i by discipline j ($25 \leq D_{X_{ij}} \leq 100$); α – summary coefficient of significance ($0 < \alpha < 1$); weight w_i={0, 1}, $P_{X_{ij}}$- total graduated result X_i of discipline j ($25 \leq P_{X_{ij}} \leq 100$); m_j – number of disciplines in curriculum training part j.

2. The indicator of psychological suitability (P_{01}^{2}) is a complex three-component qualitative indicator that combines data on the attentive, accuracy of a graduate when working with service documentation, etc. Evaluation is carried out on 5 levels: A - high, B - above average, C - medium, D - below average, E - low.

3. The level of interest in the field of information security (P_{01}^{3},%) is an assessment of the level of interest of a graduate of an educational institution based on comprehensive methods.

Unit 2 includes professional selection of applicants based on the set of obtained indicators < P_{01}^{1}, P_{01}^{2}, P_{01}^{3}>.

Unit 3 involves the formation of a readiness indicator based on the entire period of study at the university by specialty (X_1, fig. 2). The indicator takes into account the set of nominal and calculated characteristics.

Elements No. 2- No. 3 ($X_{2\text{-}3}$, fig. 2) - 'Theoretical knowledge (Practical skills)' - are composed of the level of theoretical knowledge (practical skills) (%) and the corresponding standard deviations (%).

An integral evaluation in a theoretical and practical context is a weighted average estimate. As weights, we take normalized importance factors calculated from the results of an expert survey:

$$L_t = \alpha \sum_{j=1}^{n} PN_{Cj} \cdot \sum_{i=1}^{k} dt_i^{C_j} \cdot PN_i + (1-\alpha) \cdot \sum_{j=n+1}^{n+m} PN_{Oj} \cdot \sum_{i=1}^{k} dt_i^{O_j} \cdot PN_i \quad (2)$$

$$L_p = \alpha \sum_{j=1}^{n} PN_{Cj} \cdot \sum_{i=1}^{k} dp_i^{K_j} \cdot PN_i + (1-\alpha) \cdot \sum_{j=n+1}^{n+m} PN_{Oj} \cdot \sum_{i=1}^{k} dp_i^{O_j} \cdot PN_i \quad (3)$$

where PN_i – normalized coefficient of significance of discipline *i*; PN_{Cj},PN_{Oj}- normalized coefficient of significance competency (discipline group *C* and discipline group *O*); α - coefficient of significance of competency *O*; *n*, *m* – number of competencies *C* and *O* accordingly; $dt_i^{C_j}$ and $dp_i^{O_j}$ ($dt_i^{C_j}$ and $dp_i^{O_j}$) – total result of competency *j* cycle of disciplines *C* and *O* accordingly; k_1 and k_2 – number of disciplines by realized *C* and *O* competencies; *k* – total number of disciplines.

Element No. 4 (X_4, fig. 2) - Indicator «Adequacy. Discipline».

The adequacy indicator ($X_{4(1)}$,%) determines the degree of compliance of the student with his own strength and knowledge based on the results of the state attestation exam. The discipline rate ($X_{4(2)}$,%) is a comprehensive indicator that combines the level of attendance by students in professional disciplines.

Element No. 5 (X_5, fig. 2) - Indicator of psychological suitability (pays attention to details in information security, mentally capable of handling complexity, continuously improving, honest, hardworking, stress resistance) when working with the data of a graduate of a university. Evaluation is carried out on 5 levels: A - high, B - above average, C - medium, D - below average, E - low.

The last stage of the formation of the multisociometric educational component (readiness indicator) of the information security is Stage «Employment». Based on the calculated indicators, the employer draws appropriate conclusions and makes decisions on employment or refusal of employment of a graduate of the university. Then elements (Performance data, X_6) and (Additional education, X_7) of indicator are formed.

Thus, the multisociometrical readiness characteristic represents a 7-component symbolic set of elements (mnemonic code):

$$X = < X_1, X_2, X_3, X_4, X_5, X_6, X_7 >.$$

The type of parameters of the common educational component (readiness indicator) of information security is shown in fig. 2.

The type of additional parameters of the common educational component (readiness indicator) of information security is shown in fig. 3.

7. Additional education	7.1 Additional educations last year	0000÷9999
	7.2 Number of additional educations	00÷99
	7.3 Additional specialty codes	'0'-'9'
	7.4 Numbers of professional educations	00÷99
	7.5 Scientistic degree	Yes/No/Range
	7.6 Numbers of scientistic degrees	0÷9
	7.7 Academic rank	Yes/No/Range
	7.8 Numbers of academic rank	0÷9

Figure 2: Type of additional parameters of the educational component (readiness indicator) of information security specialists

1. Specialty	1.1 Specialty code	‘0’-‘9’
	1.2 Year of graduation	0000÷9999
2. Theoretical base	2.1 Theoretical knowledge	0÷100
	2.2 Root mean square deviation	0÷100
3. Practical base	3.1 Practical skills	0÷100
	3.2 Root mean square deviation	0÷100
4. Adequacy. Discipline	4.1 Indicator of adequacy	0÷100
	4.2 Indicator of discipline level	0÷100
5. Psychological professional suitability	5.1 Psychological professional indicator 1	‘A’-‘E’
	5.2 Psychological professional indicator2	‘A’-‘E’
	5.3 Psychological professional indicator3	‘A’-‘E’
	….	
	5.*n* Psychological professional indicator n	‘A’-‘E’
6. Performance Data	6.1 Record of service	00÷99
	6.2 record of service as a specialist in the field of information security	00÷99
	6.3 Skill level	0÷9
	6.4 Rating in skill level	‘A’-‘E’

Figure 3: Type of common parameters of the educational component (readiness indicator) of information security specialists

Different information security initiatives are being carried out to improve the educational component (readiness indicator) of information security specialists. An example of quest is a game held at Novosibirsk Technical University for students of the direction of information security.

Using role-playing games for information security awareness tasks has many benefits. In addition to the clear task of simulating a real situation, we can also note the removal of psychological barriers in the interaction of players, and gaining access to practical cases that are difficult to integrate into other types of games. In recent years, there are a lot of various types of games based on the use of roles that are widely represented in information security training tasks [3-6, 9, 15]. It is important that tasks used in this types of games are usually connected in logical chains or performed in quest’s form, and also contain keys or a fixed execution scheme.

It should be noted that a large number of ethical hacking competitions are organized as Capture The Flag (CTF) in Novosibirsk Technical University. The game takes place in the digital world, while each team must protect and attack vulnerable systems and collect the flags which are alphanumeric strings. Each challenge has a description, related files or website links, 2 featuring potential hints and the amount of reward points which each participant or team collects after a successful flag submission [3-6]. Groups or individual participants are trying to collect as many reward points as possible within a certain time. The winner is the individual or the team with the most collected reward points [6].

Unit 4 is oriented to forming of standardization of every readiness indicator. If estimation of the quantitative readiness indicators does not cause the special problems because of the presence of a large

number of mathematical models, then the readiness indicators require the special attention, because the object of estimation is characterized by the large degree of uncertainties.

The aim of this block are formalization and integration of the basic data formed in the process of quality evaluation. The choice of method of construction of member functions depends on the type of the decided task, complication of receipt of the checked-up information for decision, authenticity of this information, and also from labour intensiveness of algorithm of treatment of information at the construction of member functions.

Unit 5 of the readiness index estimation algorithm assumes a standard procedure for quantitative evaluation of quantitative indicators and a fuzzy evaluation of qualitative indicators.

Example. In case of additional education (undergraduate, master's degree, higher education), reference is made in indicator 7 with indication of the cipher of the specialty (direction), after which an additional readiness indicator is formed, similar to presented before.

Note that the element "Year of the last advanced training" of component No. 7 is variable and reflects either the year of advanced training, or receiving a second education, or the assignment of a degree (title).

For example, in the case of the indicator "educational component of the IB audit" of type "090104.2005-90.10-70.15-40.95-ABAAA-4 (4) .B-2011.090900 (1) .K (1) .D (1)," one additional code is formed: "100401.2021-75.15-80.25-80.75-ABAAA" upon completion of training in the direction 100401 "Information security".

Let us first consider the first indicator:

090104.2005-90.10-70.15-40.95-ABAAA–4(4).B-2021.100401(1).K(1).D(1).

According to the described technique, component-by-component decryption yields the following results:

1. specialty - 090104.2005 ';
a. specialty code - 090104;
b. year of completion - 2005;
2. theoretical knowledge - '90.10';
a. the level of theoretical knowledge - 90%;
b. standard deviation of theoretical knowledge - 10%;
3. practical skills - 70.15 ';
a. the level of practical skills - 70%;
b. standard deviation of practical skills - 15%;
4. adequacy. discipline – '40.95';
a. adequacy - 40%;
b. discipline - 95%;
5. indicator of psychological professional suitability - "ABAAA";
a. The level of purpose is' A ';
b. Attention level - 'B';
c. Stress tolerance level - 'A';
d. Decency level - 'A';
e. The level of accuracy when working with data is'A '.
6. operation data - "4 (4) .B";
a. Work experience - 4 years;
b. Work experience in the specialty - 4 years;
c. Assessment of the manager - "B";
7. advanced training - "2021.100401 (1) .K (1) .D (1)";
a. Year of last advanced training - 2021;
b. The code of the specialty of second education is 100401;
c. The number of additional formations is 1;
d. Degree - K (candidate);
e. The number of degrees is 1;
f. Academic title - D (Associate Professor);
g. The number of scientific ranks is 1.

Next, consider a component by component additional measure of the fitness of the species:

“100401.2021-75.15-80.25-80.75-ABAAA”.

According to the described technique, component-by-component decryption yields the following results:

1. specialty - 100401.2021';
a. specialty code - 100401;
b. year of completion - 2021;
2. theoretical knowledge - '75.15';
a. the level of theoretical knowledge - 75%;
b. standard deviation of theoretical knowledge - 15%;
3. practical skills - 80.25 ';
a. the level of practical skills - 80%;
b. standard deviation of practical skills - 25%;
4. adequacy. discipline – '80.75';
a. adequacy - 80%;
b. discipline - 75%;
5. indicator of psychological professional suitability - 'ABAAA';
a. The level of purpose is' A ';
b. Attention level - 'B';
c. Stress tolerance level - 'A';
d. Decency level - 'A';
e. The level of accuracy when working with data is 'A '.

The formed indicator indicates the high educational achievements of the employee in the first specialty "Comprehensive protection of informatization objects" in the context of 90% theoretical knowledge and 70% practical skills with a small spread of 10-15% during the entire training period, as well as a high level of professional fitness (dominance of the results of the 'A' level).

Moreover, the specialist has 4 years of experience in the professional field.

The presence of an additional indicator indicates the presence of a second education in the field of information security (magistracy 100401 "Information Security"). The component composition indicates high levels of theoretical knowledge (75%) and practical skills (80%), adequacy (80%) and discipline (75%), as well as professional fitness (dominance of "A" level results).

In the end, based on a comprehensive measure of preparedness, it can be concluded that this employee is of interest to employers in the future.

4. Experimental part

The technology of formation of qualitative and quantitative indicators in the form of the information security specialist readiness as an element of a trusted environment figure has been tested in Novosibirsk technical university. Students of different specialty (10.03.01 Information security, 10.05.03 Information security of automized systems) took part in this experiment (department information security). Thus, experimental work on the formation of indicators of readiness of specialists in the field of information security was carried out in the period 2020-2021.

The formation of readiness indicator of information security specialists, interaction with employers contributed to increasing the responsibility of all participants in the educational process for the total results. The results of pedagogical monitoring were: a clearer organization of practices, improved educational programs of a number of disciplines, modified educational and methodological complexes, modernized laboratory installations.

Teachers noted the increased interest of students in the learning process. From these positions, the motivational factor for learning was investigated throughout the training period according to the modified methodology.

Dynamics of structural elements of the readiness indicator on average (levels of theoretical knowledge, practical skills) is positive. Individual psychological qualities were assessed by specialists of the professional psychological selection group using a set of psychodiagnostical methods and tests taking into account modern requirements for an information protection specialist.

The experts of the commission, when assessing the psychological qualities of specialists in the field of information security, made a conclusion on the professional suitability of graduates on the basis of levels of determination, mindfulness, stress resistance and others.

5. Conclusion

The article discusses the characteristics of Information security management. Today, conducting an audit of information security management systems is a necessary and required activity. A number of organizations whose business is closely connected with the use of information technologies, such as banks, oil, gas, energy and telecommunications companies, have recently become more active in conducting audits of information security management systems. Information security risks from personnel constitute a separate group of information security risks of the organization with a specific set of causes and conditions for their implementation. Thus in order to optimize the processes of information security audit and applicant diagnostics, there is a need to develop an educational component as a multisociometric characteristic, firstly, an indicator of the readiness of applicants as the most important factor affecting the formation of the competence of a student at the university, secondly, an indicator of the readiness of a graduate of the university for professional activities, and thirdly, an indicator of the professionalism of an information security specialist, which is the resulting component of educational activities.

The multisociometrical readiness characteristic represents a 7-component symbolic set of elements (mnemonic code): specialty, theoretical base, practical base, indicators of adequacy and discipline, psychological professional suitability indicators, performance data indicators, additional indicators.

6. Acknowledgement

This work was supported by the Vladimir Potanin Foundation for Basic Research project No GK21-001229

7. References

[1] Bilbao A. Measuring security / A. Bilbao, E. Bilbao // 47th International Carnahan Conference on Security Technology (ICCST), 2013. pp. 1-5. https://doi.org/10.1109/CCST.2013.6922054.

[2] Fernandez E. B. Measuring the Level of Security Introduced by Security Patterns / Fernandez E. B. et al // International Conference on Availability, Reliability and Security, 2010, pp. 565-568, doi: 10.1109/ARES.2010.111.

[3] Hamari, J., Koivisto, J. and Sarsa, H. (2014). Does Gamification Work? - A Literature Review of Empirical Studies on Gamification. Proceedings of the Annual Hawaii International Conference on System Sciences. 10.1109/HICSS.2014.377.

[4] Hendrix, M., Al-Sherbaz, A., Victoria, B.: Game based cyber security training: are serious games suitable for cyber security training?. International Journal of Serious Games, 3(1), 53-61 (2016). https://doi.org/10.17083/ijsg.v3i1.107.

[5] Hironori Washizaki, Security patterns: Research direction metamodel application and verification, Big Data and Information Security (IWBIS) 2017 International Workshop on, pp. 1-4, 2017.

[6] Karagiannis S. An Analysis and Evaluation of Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools / Stylianos Karagiannis, Elpidoforos Maragkos, Emmanouil Magkos // IFIP World Conference on Information Security Education, 2020. DOI: 10.1007/978-3-030-59291-2_5.

[7] Krokhaleva A. B. The human factor in the system of socially significant activity (article of the Higher Attestation Commission)/A. B. Krokhaleva, V. M. Belov//Mathematical structures and modeling. – 2017. - № 4(44). - p. 85 - 99.

[8] Monica G. Tolani. Use of artificial intelligence in cyber defence / Monica G. Tolani, Harsha G. Tolani // International Research Journal of Engineering and Technology (IRJET), 2019. pp. 3084-3087.

[9] Official website of Positive Technologies, 2021. - URL: https://www.ptsecurity.com/ru-ru/.
[10] Rajasekar A. Sociometric Methods for Relevancy Analysis of Long Tail Science Data / A. Rajasekar et al. // International Conference on Social Computing, 2013, pp. 1-6, doi: 10.1109/SocialCom.2013.6.
[11] Sahar Al-Dhahri. Information Security Management System / Sahar Al-Dhahri, Manar Al-Sarti, Azrilah Abdaziz // International Journal of Computer Applications, 2017. vol. 158 – No 7. pp. 29-33. DOI: 10.5120/ijca2017912851.
[12] Somepalli S. H. Information Security Management / Somepalli, S. H. et. al // HOLISTICA – Journal of Business and Public Administration, vol. 11, iss. 2, 2020. pp. 1-16. DOI: 10.2478/hjbpa-2020-0015.
[13] Tolani M. G. Use of artificial intelligence in cyber defense / M. G. Tolani, H. G. Tolani // International Research Journal of Engineering and Technology (IRJET), 2019. 6(7), pp. 3084-3087. URL: https://www.irjet.net/archives/V6/i7/IRJET-V6I7468.pdf.
[14] Zaydi M. A New Approach of Information System Security Governance: A Proposition of the Continuous Improvement Process Model of Information System Security Risk Management: 4D-ISS / M. Zaydi, N. Bouchaib // 27th IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE-2018) At: PSB PARIS-FRANCE, 2018, pp. 112-118. IEEE. https://doi.org/10.1109/WETICE.2018.00028.
[15] Zolotarev V. V. Strategies of social engineering attacks on information resources of gamified online education projects / V. V. Zolotarev, A. B. Arkhipova, N. Y. Parotkin, A. P. Lvova. – Text : electronic // CEUR Workshop Proceedings. – 2021. – Vol. 2861 : International Scientific Conference on Innovative Approaches to the Application of Digital Technologies in Education (SLET–2020), Stavropol, 12–13 Nov. 2020. – P. 386–391. – URL: http://ceur-ws.org/Vol-2861/. – Publication date: 13.05.2021.
[16] Zolotareva G. New approach to risk controlling in information security / G. Zolotareva, V. Zolotarev, S. Filko // Journal of Physics Conference. 2019. Series 1210(1):012170. DOI: 10.1088/1742-6596/1210/1/012170.