УДК 004.032

METHODOLOGY FOR ASSESSING THE LEVEL OF INFORMATION SECURITY OF THE EDUCATIONAL INFORMATION SYSTEM BASED ON FUZZY CLASSIFIER AND HIERARCHY OF DAMAGES

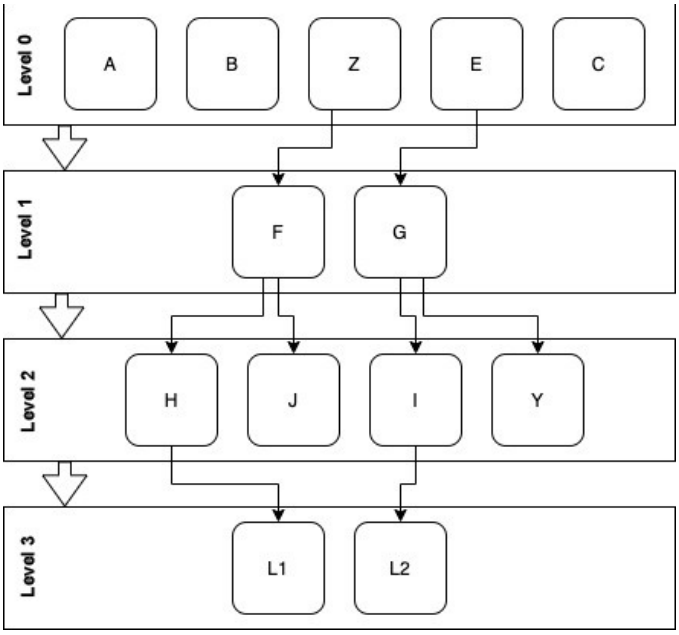
The article was received by the editorial board on 30.09.2020, in the final version – 24.10.2020.

Erkulov Bekhzod A., Navoi State Pedagogical Institute, 45 Ibn Sino St., Navoi, Uzbekistan,
Lecturer, e-mail: texnogarant@list.ru
Azhmukhamedov Iskandar M., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
Doct. Sci. (Engineering), Professor, e-mail: aim_agtu@mail.ru

The paper considers the problem of assessing the level of information security of educational information systems in the context of digital transformation of society. A methodology for determining the level of information security of educational information systems based on expert information and a knowledge base consisting of fuzzy production rules is proposed. This approach differs in that it allows formalizing qualitative assessments of the state of the system using the theory of fuzzy sets and assessing the level of information security of educational information systems not only in real time, but also at the stage of their development and implementation. Also, the technique involves building a hierarchy of system damage, which can impede the identification of each other. The implementation of the methodology makes it possible to increase the efficiency of the quality management process of educational information systems and the educational process as a whole.

Keywords: educational system, quality of information systems, digitalization of education, information security of the educational information system

Графическая аннотация (Graphical annotation)



МЕТОДОЛОГИЯ ОЦЕНКИ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ НЕЧЕТКОГО КЛАССИФИКАТОРА И ИЕРАРХИИ ПОВРЕЖДЕНИЙ

Статья поступила в редакцию 30.09.2020, в окончательном варианте – 24.10.2020.

Ёркулов Бехзод Абдугаббарович, Навоийский государственный педагогический институт, Узбекистан, г. Навои, ул. Ибн Сино, 45,
преподаватель кафедры методики преподавания информатики, e-mail: texnogarant@list.ru
Ажмухамедов Искандар Маратович, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
доктор технических наук, профессор кафедры информационной безопасности, e-mail: aim_agtu@mail.ru

В статье рассматривается проблема оценки уровня информационной безопасности образовательных информационных систем в условиях цифровой трансформации общества. Предлагается методика определения уровня информационной безопасности образовательных информационных систем на основе экспертной информации и базы знаний, состоящей из нечетких продукционных правил. Этот подход отличается тем, что позволяет формализовать качественные оценки состояния системы с использованием теории нечетких множеств и оценить уровень информационной безопасности образовательных информационных систем не только в режиме реального времени, но и на этапе их создания, разработки и внедрения. Также методика предполагает построение иерархии повреждений системы, которые могут препятствовать их идентификации. Внедрение методики позволяет повысить эффективность процесса управления качеством образовательных информационных систем и образовательного процесса в целом.

Ключевые слова: образовательная система, качество информационных систем, цифровизация образования, информационная безопасность образовательной информационной системы

LEVELS OF HIERARCHY

Introduction. The trend towards digitalization of all spheres of society, undoubtedly, has become a prerequisite for the introduction of electronic technologies in the field of education. And if at the dawn of the new technical revolution "digital" penetrated the higher education system, then the 2020 were marked by the digitalization of secondary schools as a kind of addition to the traditional one. After 2018, the paradigm of active implementation of online courses has strengthened in higher educational institutions, including the practice of replacing (on an alternative or non-alternative basis) traditional disciplines by distance learning. These practices provoked heated discussions, since not all disciplines turned out to be meaningfully and methodically adaptable to the online format. However, no one considered the option of a complete transition "to digital" as the only correct one.

The problems caused by the coronavirus pandemic have affected all areas of public life, including education. If earlier mainly higher educational institutions, interested in reaching the audience and implementing projects of lifelong and accessible education, gravitated towards the remote conduct of the educational process, then forced self-isolation has led to the fact that distance technologies, which are poorly demanded by the school, have become an urgent need. The massive transition of all schools to online education clearly demonstrated the problem of assessing the level of information security of educational information systems, the relevance of which was missed in "peacetime", since an increase in the load on these systems led to various negative consequences, for example, educational portals that were not designed for a one-time stay of a large number of users did not cope with the load and errors occurred, as a result of which students could not receive the assignment. The number of hacker attacks on educational systems has also frighteningly increased, in connection with this there is an urgent need to assess the state of the educational information systems (EIS) for information security, while such an assessment must be carried out constantly as part of the quality management of the EIS [3].

Fuzzy damage assessment classifier. During the analysis of the subject area, it was revealed that the current level of information security of the EIS is directly related to the intensity of damage to information assets and information protection means (IPM). Their level is most often determined by the decision-maker by tracking changes and assessed verbally [6].

To formalize linguistic assessments of damage to information assets and IPM, we introduce the linguistic variable "Parameter value" and assign it to the term-set of its values VP, which will consist of 9 elements belonging to the positive or negative range of assessments:

VP = {Extremely negative (A^-); Above average negative (B^-); Medium negative (C^-); Low negative (D^-); Null (0); Low positive (D^+); Medium positive (C^+); Above average positive (B^+); Overwhelmingly positive (A^+)}

For the graphical representation of VP, a nine-level classifier has been compiled, within the framework of which trapezoids are assigned to the membership functions of fuzzy numbers on the segment $[-1, 1] \in R$:

$$\{A^-(-1; -1; -0{,}85; -0{,}75); B^-(-0{,}85; -0{,}75; -0{,}65; -0{,}55); C^-(-0{,}65; -0{,}55; -0{,}45; -0{,}35);$$
$$D^-(-0{,}45; -0{,}35; -0{,}25; -0{,}15); «0»(-0{,}25; -0{,}15; 0{,}15; 0{,}25);$$
$$D^+(0{,}15; 0{,}25; 0{,}35; 0{,}45); C^+(0{,}35; 0{,}45; 0{,}55; 0{,}65);$$
$$B^+(0{,}55; 0{,}65; 0{,}75; 0{,}85); A^+(0{,}75; 0{,}85; 1;1)\},$$

where in a fuzzy number $XX(a_1, a_2, a_3, a_4)$ a_1 and a_4 – abscissa of the lower base, a_2 and a_3 – abscissa of the upper base of the trapezoid.

It is important to note that the sum of all membership functions for any $x \in [-1, 1]$ must be equal to one to ensure consistency.

The advantage of such a fuzzy classifier is that if nothing is known about the parameter, except that its value can be in the interval [–1, 1]. In addition, the classifier is convenient for the association between

qualitative and quantitative estimates of the parameter with the maximum highest results. It is a kind of modification of the "gray" scale of D.A. Pospelova [8], which is a scale with smooth transitions between properties, in contrast to the interval scale, where the transitions occur abruptly. In the world scientific community, it is believed that smooth "gray" scales more clearly reflect expert assessments and the specifics of decision-making in conditions of uncertainty [7–9].

The proposed classifier makes it possible to move from a verbal linguistic assessment to a smooth interval scale with symmetric classification nodes in a consistent manner. In this node, the function value is equal to 1, in the rest – to zero. With distance from the node or approaching it, the expert decreases or increases the degree of confidence in classification and assessment.

It is important to note that the number of classifier levels depends on the requirements for the accuracy of the assessment and the expert's opinion. Binary (yes, no, good or bad) or ternary (high, medium, low) classifiers are often used, however, in our opinion, they are not accurate enough to determine the quality of the EIS.

Formalization of expert judgments about the amount of damage. In order to formalize expert judgments, reflecting the impact of the detected damage to information assets and IPM on the level of information security services, it is proposed to apply a set of fuzzy production rules of the form (1), which represent a knowledge base (KB):

$$\text{IF } (\&_{i=1}^{N}[\text{Pov}_i == P_i]) \text{ Then } (\&_{j=1}^{M}[(O_j)(K_j == S_j)]), \quad (1)$$

where $P_i, S_j \in$ VP – linguistic assessments of the levels of damage to assets and IPM and assessments of the state of IS characteristics; symbol «= =»acts as an operator for comparing two values; terms "$\text{Pov}_i = P_i$" express the level of the i-th damage to an asset or IPM; consequence "$K_j == S_j$" determines the state of the j-th security service; O_j reflects the degree of confidence of the expert in the investigation, and according to the Harrington metric has the following verbal relations: 0,00–0,19 – the probability is extremely low; 0,20–0,36 – probability is low; 0,37–0,63 – average probability; 0,64–0,79 – the probability is high; 0,80–1,0 – the probability is extremely high.

Revealing the damage hierarchy. In the process of filling the knowledge base, a situation is widespread when, with a high level of some damage, it becomes difficult to identify the level of others (for example, with a high level of physical damage to the device, it is not possible to establish the amount of software damage).

In order to systematize this fact, a hierarchy of injuries was formulated, consisting of 4 levels (fig. 1).

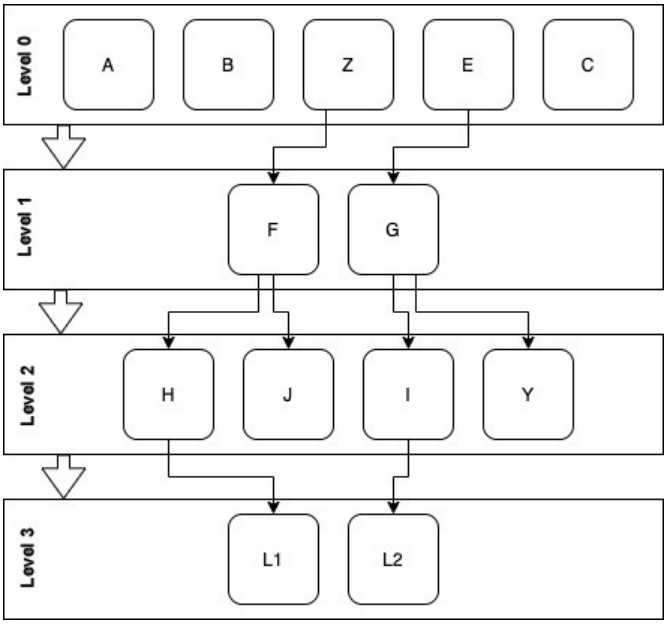


Figure 1 – Hierarchy of damage to assets and IPM

The zero level includes:

1. Damage to information transmission channels. They affect the integrity, availability and reliability of data (A).

2. Physical damage to the structural components of the servers. They affect the integrity, availability and validity of data (Z).

3. Physical damage to the structural components of workstations. They affect the integrity, availability and reliability of data (E).

4. Damage to independent structural components of IPM: technical engineering and hardware means; organizational and legal measures to protect information. They affect the confidentiality, integrity, availability and reliability of data (B).

5. Damage to media with data backups. This damage affects the availability, reliability and integrity of information (C).

The first level includes:

6. Damage to the system software of the servers. They affect the integrity, availability and reliability of data (F).

7. Damage to the system software of workstations. They affect the integrity, availability and reliability of data (G).

The second level includes:

8. Damage to the server application software (H). They affect the integrity, availability and reliability of data.

9. Damage to the application software of workstations. They affect the integrity, availability and validity of data (I).

10. Damage to software information security systems on servers. They affect the confidentiality, integrity, availability and reliability of data (J).

11. Damage to software information security systems on workstations. They affect the confidentiality, integrity, availability and reliability of data (Y).

The third level includes:

12. Damage to files on servers. They affect the integrity, availability and validity of data (L1).

13. Damage to files on workstations. They affect the integrity, availability and reliability of data (L2).

A hierarchical system of possible damage to structural components built in this logic satisfies the following conditions:

- within the same hierarchical level, damages do not affect each other;
- damages located at lower levels of the hierarchy are capable of influencing the detection of damages at higher levels.

Each of the levels of the hierarchical structure of possible damage, if desired, can be decomposed, but only under strict fulfillment of the above conditions.

In order to form a knowledge base, experts define the following rules [1]:

$$\text{IF } [\text{Pov}_i == D_i] \text{ Then } (O_i\ (K_j == S_i)], \quad (2)$$

The rules formulated in this way express the influence of each level of damage to components in blocks of the hierarchical structure on information security services.

Because the level of possible damage is characterized by values from the right side of the nine-level VP classifier, then for each of the 5 expressed values, it is required to formulate 4 rules (1 rule for each of the IS services, which may be affected by these damages). Thus, the number of rules for each possible damage included in the hierarchical block is 20. The total number of rules in the knowledge base is 415 pieces.

It is important to note that the knowledge base formulated in this way is:

- complete, because there is a logical conclusion for each possible damage and level of the hierarchical structure of damage;
- irredundant, because the absence of at least one of the rules leads to incomplete information in the knowledge base;
- consistent, since there is no situation in which two rules have the same left-hand side with different right-hand sides.

Definitely an important stage in the development of the KB is the formulation of a list of "key" damages and their "critical" levels. Key damages when reaching their critical level prevent the identification of damage to components of the next level of the hierarchy. As part of an expert assessment, it is required to identify “critical” levels of “key” damage to elements at each hierarchical level.

Level zero is characterized by the following "key" injuries:

- physical damage to EIS servers, which in case of “critical” damage do not allow identifying damage of the first, second and third levels;
- physical damage to workstations that are part of the EIS, which in case of "critical" damage do not allow identifying damage of the first, second and third levels.

The first level is characterized by the following "key" injuries:

- damage to the system software of EIS servers, which in case of “critical” damage do not allow identifying damage of the second and third levels;

- damage to the system software of workstations that are part of the EIS, which, in case of "critical" damage, do not allow identifying damage of the second and third levels.

The second level is characterized by the following "key" injuries:

- damage to the application software of the EIS servers, which, in case of “critical” damage, do not allow identifying damage of the third level;
- damage to the application software of workstations that are part of the EIS, which, in case of "critical" damage, do not allow identification of damage of the third level.

Methodology for assessing the level of information security of an educational information system. The procedure for assessing the level of information security in the EIS can be represented as an iterative block diagram (fig. 2), which reflects the following stages:

1. Finding a matching rule in the KB.
2. Assessment of information security services at the considered hierarchical level according to the rules from the KB.
3. Placing and removing blocks that have critical critical damage.
4. Calculation of the integrated assessment of services and the general indicator of the information security of the EIS.

Assessment of the state of information security services at each hierarchical level requires the development of a procedure for using KB rules. Its input parameters are qualitative assessments of damage to information resources and IPM at the considered hierarchical level. On this basis, the search for KB rules is carried out and by formulating the rules below, the level of influence of damage to each element of the hierarchy on information security services is revealed:

$$K_j^k: \text{IF } (\&_{i=1}^{W}[Pov_i = P_i]). \text{ Then } (\&_{j=1}^{N}[\max_m O_{m\ m\in \arg\min_i S_i} \quad K_j^k = \min_i S_i\ )), \qquad (3)$$

where k – hierarchical block number; K_j^k – j-th information security service, characterizing the k-th block; W – number of damages in the k-th block; P_i – level of detected damage Pov_i; N – number of information security services, affected by damage to the k-th block; S_i is the value of the information security service K_j determined according to the existing database rules at the damage level Pov_i equal to P_i; O_m – the degree of an expert's confidence in assessing the impact of damage Pov_i, having a level P_i, on the j-th information security service.

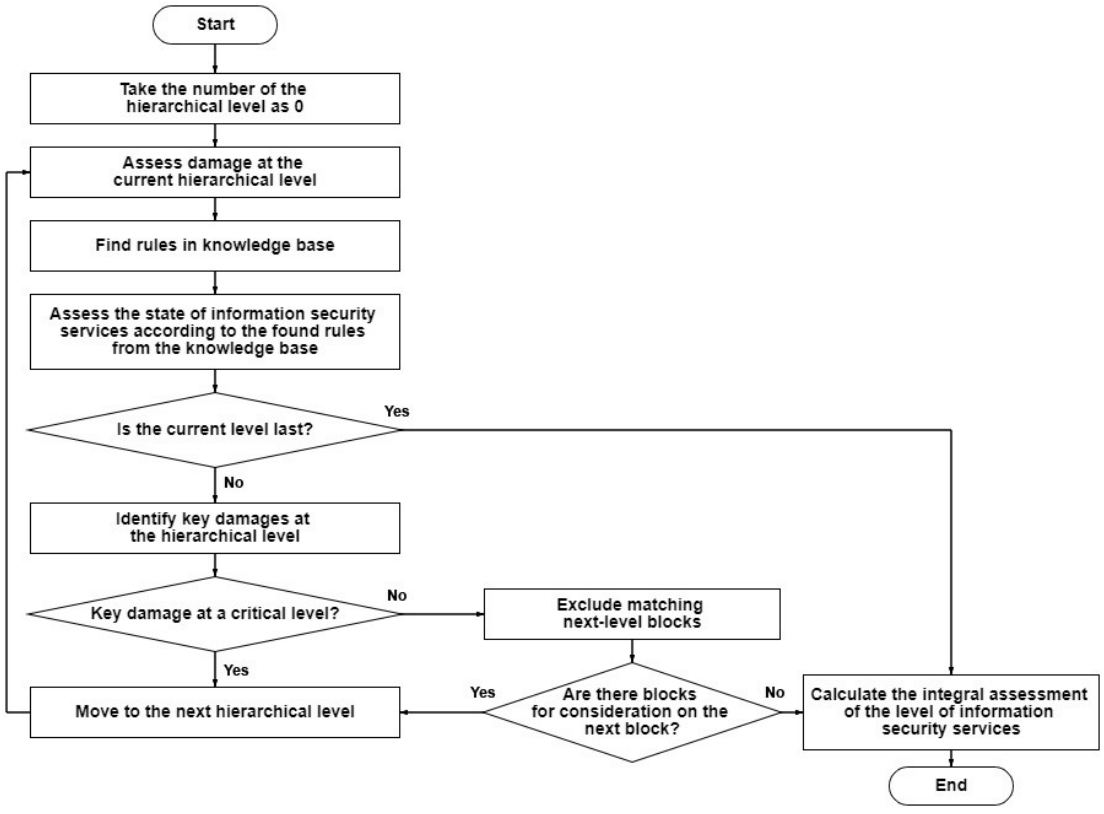


Figure 2 – Algorithm for calculating the information security indicator of the EIS

As part of the calculation of the indicator of the level of information security, OIS are generated automatically:

- at the 0-th hierarchical level of damage: 5 block rules;
- at the 1-st hierarchical level of damage: up to 2 rules;
- at the 2-nd hierarchical level of damage: up to 4 rules;
- at the 3-rd hierarchical level of damage: up to 2 rules.

The estimate of the value of information security services at each hierarchical level is calculated as the minimum value obtained as a result of using the generated block rules of the analyzed level:

$$K_j^l: \max_m O_{m \in \arg\min_k K_j^k} \quad [K_j^l = \min_k K_j^k], \tag{4}$$

where K_j^l – is the j-th security service at the l-th level.

The algorithm described in this way for determining the state of information security services at each hierarchical level with the formation of an automatic rule makes it possible to simplify the filling of the KB. In addition, it allows to reduce the complexity of the KB modification when it is necessary to delete, add or edit production rules, because block rules are subject to formation only at the time of assessing the level of information security.

The integral assessment of information security services K_j is defined as the minimum value of the information security criteria identified at each of the hierarchical levels that were found:

$$K_j: \max_m \{O_m\}_{m \in \{\arg(\min_l K_j^l)\}} [K_j = \min_l K_j^l], \tag{5}$$

It is important to note that in the case of a separate analysis of the level of information security separately from the EIS quality management process, the decision maker can calculate a generalized information security indicator based on an additive convolution of previously obtained integral estimates:

$$K_0 = \sum_{j=1}^{n} \alpha_j \cdot K_j, \tag{6}$$

where K_0 is a generalized indicator of information security of the EIS as a whole; n is the number of considered properties of information; $\alpha_j \in [0; 1]$ is the coefficient of influence of K_j on K_0, $\sum_j^n \alpha_j = 1$.

In order to determine the value of the coefficients of the influence of information properties when calculating the generalized indicator of the level of information security of the OIS, it is advisable to use a modified method of non-strict ranking, in accordance with which the decision maker enumerates the properties of information to increase the degree of their significance (criticality). At the same time, it is believed that the decision maker can assign the same degree of significance to several properties. In such a situation, the decision maker places them side by side arbitrarily. The rank of the evaluated properties is determined by their number. The property estimates calculated in this way are generalized Fishburne weights with a mixed distribution of preferences.

Conclusion. Thus, the proposed methodology for assessing the current level of information security of EIS in comparison with the existing analogues takes into account the impact of damage to information resources and information security systems on each other within hierarchical levels, as well as qualitative expert assessments of damage states. At the same time, the proposed technique, with proper adaptation, can be applied to any systems and assessments, for example, when assessing the level of operational safety, fire safety, etc.

References

1. Azhmukhamedov I. M., Protalinsky O. M. Metodologiya modelirovaniya plokho formalizuemykh slabo strukturirovannykh sotsiotekhnicheskikh sistem [Methodology for modeling poorly formalized poorly structured socio-technical systems]. *Vestnik AGTU. Seriya: Upravlenie, vychislitelnaya tekhnika i informatika* [Bulletin of ASTU. Series: Management, computer technology and informatics], 2013, no. 1, pp. 144–154.

2. Azhmukhamedov I. M. *Informatsionnaya bezopasnost. Sistemnyy analiz i nechetkoe kognitivnoe modelirovanie : monografiya* [Information Security. System analysis and fuzzy cognitive modeling : monograph]. Moscow, LAP LAMBERT Academic Publishing GmbH & Co. KG; Astrakhan, 2012. 385 p.

3. Glukhova L. V. Metodologiya otsenki i upravleniya kachestvom funktsionirovaniya informatsionnykh sistem [Methodology for assessing and managing the quality of information systems functioning]. *Vestnik Kazanskogo tekhnologicheskogo universiteta* [Bulletin of Kazan Technological University], 2008, no. 4, pp. 174–181.

4. Eppler M., Wittig D. Conceptualizing information quality: A review of information quality frameworks from the last ten years. *Proceedings of the 2000 Conference on Information Quality*. Boston, M.I.T., 2000, pp. 83–91.

5. Kuznetsov O. P. *Kognitivnoe modelirovanie slabo strukturirovannykh situatsiy* [Cognitive modeling of poorly structured situations]. Available at: http://posp.raai.org/data/posp2005/Kuznetsov/kuznetsov.html (accessed 12.28.2016).

6. Prieto-Diaz R. *The Common Criteria Evaluation Process: Process Explanation, Shortcomings, and Research Opportunities.* Harrisonburg, Virginia, James Madison University, USA, December 2002. 56 p. (Technical Report Series; CISC-TR-2002-03. Version 1.0.2/Commonwealth Information Security Center).

7. Rao P. P. B., Shankar N. R. Ranking generalized fuzzy numbers using area, mode, spreads and weight. *International Journal of Applied Science and Engineering*, 2012, vol. 1, no. 10, pp. 41–57.

8. Pospelov D. S. «Serye» i / ili «chyorno-belye» [shkaly] ["Grey" and / or "black and white" [scales]]. *Prikladnaya ergonomika. Spetsvypusk «Refleksivnye protsessy»* [Applied ergonomics. Special issue "Reflexive Processes"], 1994, no. 1, pp. 26–39.

9. Yarushkina N. G. *Nechyotkie gibridnye sistemy. Teoriya i praktika* [Fuzzy hybrid systems. Theory and practice]. Moscow, Fizmatlit Publ., 2007. 208 p.

Библиографический список

1. Ажмухамедов И. М. Методология моделирования плохо формализуемых слабо структурированных социотехнических систем / И. М. Ажмухамедов, О. М. Проталинский // Вестник АГТУ. Сер. Управление, вычислительная техника и информатика. – 2013. – № 1. – С. 144–154.

2. Ажмухамедов И. М. Информационная безопасность. Системный анализ и нечеткое когнитивное моделирование: монография / И. М. Ажмухамедов. – Москва : LAP LAMBERT Academic Publishing GmbH & Co. KG. ; Астрахань, 2012. – 385 с.

3. Глухова Л. В. Методология оценки и управления качеством функционирования информационных систем / Л. В. Глухова // Вестник Казанского технологического университета. – 2008. – № 4. – С. 174–181.

4. Eppler M., Wittig D. Conceptualizing information quality: A review of information quality frameworks from the last ten years // Proceedings of the 2000 Conference on Information Quality. – Boston : M.I.T., 2000. – P. 83–91.

5. Кузнецов О. П. Когнитивное моделирование слабо структурированных ситуаций / О. П. Кузнецов. – Режим доступа: http://posp.raai.org/data/posp2005/Kuznetsov/kuznetsov.html, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 28.12.2016).

6. Prieto-Diaz R. The Common Criteria Evaluation Process: Process Explanation, Shortcomings, and Research Opportunities / R. Prieto-Diaz. – Harrisonburg, Virginia : James Madison University, USA, December 2002. – 56 p. – (Technical Report Series; CISC-TR-2002-03. Version 1.0.2/Commonwealth Information Security Center).

7. Rao P. P. B. Ranking generalized fuzzy numbers using area, mode, spreads and weight / P. P. B. Rao, N. R. Shankar // International Journal of Applied Science and Engineering. – 2012. – Vol. 1, № 10. – P. 41–57.

8. Поспелов Д. С. «Серые» и / или «чёрно-белые» [шкалы] / Д. С. Поспелов // Прикладная эргономика. Спецвыпуск «Рефлексивные процессы». – 1994. – № 1. – С. 26–39.

9. Ярушкина Н. Г. Нечёткие гибридные системы. Теория и практика / Н. Г. Ярушкина. – Москва : Физматлит, 2007. – 208 с.