ISSN 1815-4840, E-ISSN 2181-1105
Himičeskaâ tehnologiâ. Kontrol′ i upravlenie
CHEMICAL TECHNOLOGY.
CONTROL AND MANAGEMENT
2020, №4 (94) pp.64-70
International scientific and technical journal
*journal homepage: https://uzjournals.edu.uz/ijctcm/*
Since 2005

**UDC 004.056**

# RELIABLE RISK ASSESSMENT METHOD FOR EFFECTIVE ORGANIZATION OF INFORMATION SECURITY AT ENTERPRISE

**Botirov Fayzullajon Bakhtiyorovich**[1]

*Tashkent University of Information Technologies named after Muhammad al-Khwarizmi*
*Address: 118, Amir Temur st., 100095, Tashkent city, Republic of Uzbekistan*
*E-mail: botirov_fz@mail.ru, Phone:+998-97-751-16-97*

***Abstract:*** *The problems of the new industry 4.0 automation paradigm are considered and the latest technologies in the field of information and communication technologies that stimulate it are analyzed, including cyber-physical systems, cloud computing, the Internet of things and big data. Some methods of multidimensional, multi-faceted industrial representation and analysis of big data are proposed. The basics of big data processing using granular computing methods have been developed. Marked the emergence of the problem of creation of special cognitive tool for constructing artificial agents, understanding integrated intelligence enterprises. In the process of information protection at the enterprise, it is proposed to optimize the information system of the enterprise and implement a protection mechanism for each part, as well as to group the risks for information in this system in a distributed information system.*

***Keywords:*** *HAM, intellectual information system, threat, vulnerability, matrix.*

***Аннотация:*** *Автоматлаштиришнинг янги парадигмаси бўлган Industry 4.0 нинг муаммолари кўриб чиқилгна ҳамда унинг ахборот ва коммуникация технологиялари, жумладан, киберфизик тизимлар, булутли ҳисоблаш, Интернет буюмлари ва катта ҳажмли маълумотларни рағбатлантириш соҳасидаги энг янги технологиялар таҳлил қилинган. Катта ҳажмли маълумотларни кўп ўлчамли, кўп қиррали саноатли акс эттириш ва таҳлил қилишнинг бир қанча усуллари таклиф этилган. Гранулали ҳисоблаш усулидан фойдаланиб, катта ҳажмли маълумотларга ишлов бериш асослари ишлаб чиқилган. Интеграллашган интеллектуал корхоналар учун тушунишнинг сунъий агентларини қуришни махсус когнитив воситаларини яратиш муаммолари юзага келганлиги кўрсатилган. Корхонада ахборотларни ҳимоялаш жараёнида корхонани ахборот тизимини оптималлаштириш ҳамда ҳар бир қисм учун ҳимоя механизмини амалга ошириш, шунингдек мазкур тизим учун ахборотлар хавфини тақсимланган ахборот тизимида гуруҳлаш таклиф этилган.*

***Таянч сўзлар:*** *интеллектуал ахборот тизими, таҳдид, заифлик, матрица.*

***Аннотация:*** *Рассмотрены проблемы новой парадигмы автоматизации Industry 4.0 и проанализированы новейшие технологии в области стимулирующих ее информационных и коммуникационных технологий, включая киберфизические системы, облачные вычисления, Интернет вещей и большие данные. Предложены некоторые способы многомерного, многогранного промышленного представления и анализа больших данных. Разработаны основы обработки больших данных с использованием методов гранулярных вычислений. Отмечено возникновение проблемы создания специальных когнитивных инструментов построения искусственных агентов понимания для интегрированных интеллектуальных предприятий. В процессе защиты информации на предприятии предлагается оптимизировать информационную систему предприятия и реализовать механизм защиты для каждой части, а также сгруппировать риски для информации в этой системе в распределенной информационной системе.*

***Ключевые слова:*** *интеллектуальная информационная система, угроза, уязвимость, матрица.*

## Introduction

In order to effectively protect against information security threats within the enterprise intelligent information system, it is necessary to determine what types of threats to this information exist during the information life cycle. Because each enterprise is unique and there is no static information on threats to protected objects, information security threats at different stages of the life cycle, it is necessary to use heuristic methods or expert assessment methods to determine what types of threats exist [1].

## Main part

Reliable risk assessment is a guarantee of effective organization of information protection. However, there are no well-established methods of estimating the calculation of parameters that determine information risks. This is due to a number of reasons:

1. The need to take into account when assessing the risk of relevant factors that are qualitative and do not have elementary measurement properties;
2. The need to include destructive models in the process of assessing risk factors with its goals, motives, holding factors. Incompleteness and inaccuracy of the corresponding intruder model reduces the accuracy of the risk analysis;
3. The need to ensure the accuracy and consistency of the emerging assessments of risk;
4. Ability to quantify the final risk estimates for further analytical processing.

The processing of the obtained values is required to be carried out by the method of hierarchical analysis. The basis of the method is the construction of a multi-level hierarchy through the decomposition of factors affecting the final goal [2]. Factors spread across different levels of the hierarchy. The relationship between the factors determines their interdependence in the object under consideration. The result of the construction of the hierarchy is to determine the degree of influence of each factor on the final goal.

The advantage of the method is as follows:

- Possibility to use linguistic variables as expert assessments;
- Possibility to include the advantages of the intruder model in the calculation process;
- the ability to evaluate parameters with different scales of incompatibility.

The application of the hierarchical analysis method (HAM) to calculate the threat level provides an opportunity to identify and analyze the level of impact of each information security threat in addition to the threat level indicators. In this case, each threat is analyzed by the frequency of occurrence during the year [2-4]. Once the frequency of threats is determined, it will be possible to focus protective measures on mitigating the most dangerous threat, thereby effectively reducing the risk of damage to the protected object. Figure 1 shows an overview of the information flow model.

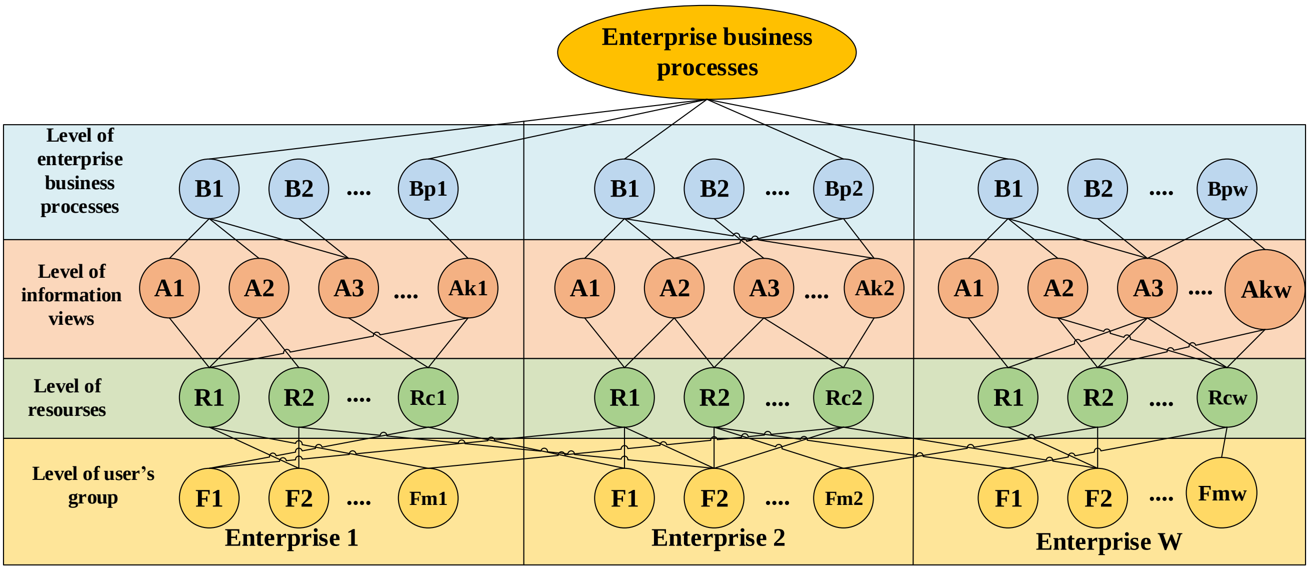

*Figure 1.* ***Information flow model in the intellectual information system of the enterprise.***

The model has the appearance of a hierarchy consisting of the following levels:

- user group level;

- level of resources;
- level of information views;
- level of business processes of the enterprise.

The individual lines in the model are the relationships that make up an enterprise's information processes. The model is built in two stages. In the first stage, security experts and enterprise managers build a model of information flows for their enterprises without taking into account the impacts on other participants in a particular enterprise.  Then, as a separate model is built, it is added to the level of business processes of the enterprise intelligent information system, as well as additional links between enterprises at the level of resources and user groups. It will then be ready for evaluation. Once again, the purpose of evaluating the information flow model is to determine the cost of the enterprise's intelligent information system resources. In the model, the resource is understood as the nodes of the intellectual information system of the enterprise: servers, computers, databases - physical objects in which information assets are stored. Evaluation is carried out on the criteria of value of objects of each level using the method of hierarchical analysis [5].

$$B = \begin{pmatrix} 1 & {}^{b_1}/_{b_2} & \dots & {}^{b_1}/_{b_n} \\ {}^{b_2}/_{b_1} & 1 & \dots & {}^{b_2}/_{b_n} \\ \vdots & \vdots & \dots & \vdots \\ {}^{b_n}/_{b_1} & {}^{b_n}/_{b_2} & \dots & 1 \end{pmatrix}, \tag{1}$$

where B is a matrix of business processes pair comparison by price criterion.

$$B_{\text{c}} = \begin{pmatrix} b_1^{\text{c}} \\ b_2^{\text{c}} \\ \vdots \\ b_n^{\text{c}} \end{pmatrix}, \tag{2}$$

where, $B_c$-B is the normalized eigenvector of the priority matrix.

$$\forall\, b_i \in B, \qquad i = 1, 2, \dots . n:$$

$$A_i = \begin{pmatrix} 1 & {}^{a_1}/_{a_2} & \dots & {}^{a_1}/_{a_k} \\ {}^{a_2}/_{a_1} & 1 & \dots & {}^{a_2}/_{a_k} \\ \vdots & \vdots & \dots & \vdots \\ {}^{a_k}/_{a_1} & {}^{a_k}/_{a_2} & \dots & 1 \end{pmatrix}, \tag{3}$$

where $A_i$ is the dual comparison matrix of information views.

$$A_{\text{c}} = \begin{pmatrix} a_1^1 & a_1^2 & \dots & a_1^n \\ a_2^1 & a_2^2 & \dots & a_2^n \\ \vdots & \vdots & \dots & \vdots \\ a_k^1 & a_k^2 & \dots & a_k^n \end{pmatrix}, \tag{4}$$

where $A_c$-A is a matrix of normalized special vectors of the dominance matrix.

$$\forall\, a_j \in A, \qquad j = 1, 2, \dots . k:$$

$$R_j = \begin{pmatrix} 1 & {}^{r_1}/_{r_2} & \dots & {}^{r_1}/_{r_s} \\ {}^{r_2}/_{r_1} & 1 & \dots & {}^{r_2}/_{r_s} \\ \vdots & \vdots & \dots & \vdots \\ {}^{r_s}/_{r_1} & {}^{r_s}/_{r_2} & \dots & 1 \end{pmatrix}, \tag{5}$$

where R$_j$ is the resource pair matrix.

$$R_c = \begin{pmatrix} r_1^1 & r_1^2 & \dots & r_1^k \\ r_2^1 & r_2^2 & \dots & r_2^k \\ \vdots & \vdots & \dots & \vdots \\ r_s^1 & r_s^2 & \dots & r_s^k \end{pmatrix}, \qquad (6)$$

where R$_c$-R is the matrix of normalized eigenvectors of the matrix of usability.

$\forall\, r_v \in R, \qquad v = 1, 2, \dots. s$:

$$F_v = \begin{pmatrix} 1 & {n_1}/{n_2} & \dots & {n}/{n_m} \\ {n_2}/{n_1} & 1 & \dots & {n_2}/{n_m} \\ \vdots & \vdots & \dots & \vdots \\ {n_m}/{n_1} & {n_m}/{n_2} & \dots & 1 \end{pmatrix}, \qquad (7)$$

where F$_v$ is the user group pair comparison matrix.

$$F_c = \begin{pmatrix} n_1^1 & n_1^2 & \dots & n_1^s \\ n_2^1 & n_2^2 & \dots & n_2^s \\ \vdots & \vdots & \dots & \vdots \\ n_m^1 & n_m^2 & \dots & n_m^s \end{pmatrix}, \qquad (8)$$

where F$_c$-F is a matrix of normal vectors with normalized matrix of preferences.

$$F_c = \begin{pmatrix} \sum_{j=1}^{n}\sum_{i=1}^{k} C_K * b_j^c * & a_i^c * & r_1^c \\ \sum_{j=1}^{n}\sum_{i=1}^{k} C_K * b_j^c * & a_i^c * & r_2^c \\ \vdots & \vdots & \vdots \\ \sum_{j=1}^{n}\sum_{i=1}^{k} C_K * b_j^c * & a_i^c * & \dots r_s^c \end{pmatrix}, \qquad (9)$$

$$C_{F_q} = \sum_{j=1}^{n}\sum_{i=1}^{k}\sum_{r=1}^{s} C_K * b_j^c * a_i^c * r_r^c * n_q^c. \qquad (10)$$

First of all, business processes that are part of the enterprise are compared in terms of value. The cross-comparison matrix B (1) is constructed for business processes, the result of the calculation of the private vector is the business process advantage vector B$_c$ (2). For each business process, a comparison is made on the value of all views of the A$_i$ information entered into it. As a result of evaluating the appearance of information, we obtain the A$_c$ matrix, which consists of column-vectors, which characterizes the predominance of different forms of information in relation to this or that business process. The information is then analyzed to place it on the resource for each view. R$_j$ is a matrix of comparisons on the value of the information (5) located in the resource, and accordingly R$_c$ (6) is the priority vector. The value of the information contained in each specific resource is calculated according to formula (9). Using the current model, the value of the information in each resource of the enterprise information system is calculated, giving the cost of a particular business process. For ease of valuation, it is necessary to determine the value of its business processes in advance, separately within each enterprise. Usually this is easy enough to do because the business has a guide to information about the benefits that different aspects of its activities bring. A separate enterprise-wide assessment simplifies the assessment procedure for experts and significantly reduces the maturity of matrices [5-6-7].

The user group level is included in the model for its completeness in context. This level is not used during the operation of an automated information security management system. However, security administrators can identify the group of users with access to the most valuable information by evaluating this level using expressions (7), (8), (10). This may be the basis for strengthening information protection management measures against employees of the enterprise belonging to this group. Taking resource value assessments, we move on to the threat and vulnerability analysis model.

The purpose of analyzing this model is to determine the level of threat to information resources. An overview of the threat and vulnerability model is shown in Figure 2.

The threat and vulnerability model includes the following levels: the level of enterprise business processes; level of information views; level of resources; level of threats and vulnerabilities. The analysis of this model is also carried out by the method of hierarchy analysis. A pair of comparison matrices is constructed for each level of the model. Based on the vectors of priorities obtained, the assessment of the level of threats to the information security of the enterprise.

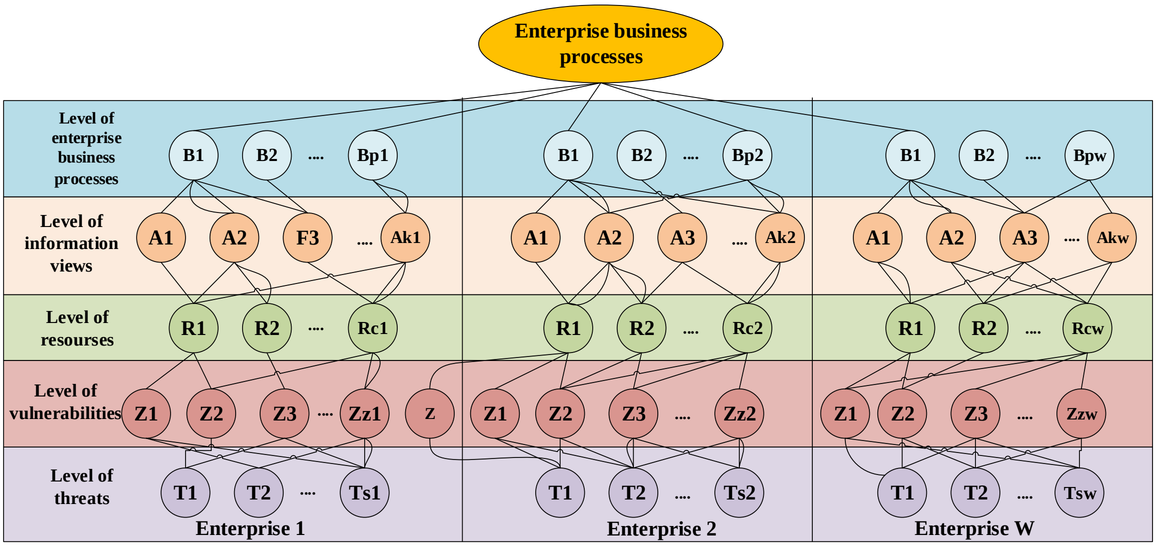

*Figure 2.* ***A model of threats and vulnerabilities in an enterprise integrated information environment.***

$$T = \begin{pmatrix} 1 & {}^{t_1}/_{t_2} & \cdots & {}^{t_1}/_{t_x} \\ {}^{t_2}/_{t_1} & 1 & \cdots & {}^{t_2}/_{t_x} \\ \vdots & \vdots & \cdots & \vdots \\ {}^{t_x}/_{t_1} & {}^{t_x}/_{t_2} & \cdots & 1 \end{pmatrix}, \tag{11}$$

where T is a double comparison matrix of threats.

$$T_c = \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_x \end{pmatrix}, \tag{12}$$

where T$_c$-T are the specific vectors that normalize the matrix of preferences.

$\forall\, t_a \in T, \qquad a = 1, 2, \dots .x:$

$$Z_v = \begin{pmatrix} 1 & {}^{z_1}/_{z_2} & \cdots & {}^{z_1}/_{z_n} \\ {}^{z_2}/_{z_1} & 1 & \cdots & {}^{z_2}/_{z_n} \\ \vdots & \vdots & \cdots & \vdots \\ {}^{z_n}/_{z_1} & {}^{z_n}/_{z_2} & \cdots & 1 \end{pmatrix}, \tag{13}$$

where Z$_v$ is the weaknesses pair matrix.

$$Z_c = \begin{pmatrix} z_1^1 & z_1^2 & \cdots & z_1^x \\ z_2^1 & z_2^2 & \cdots & z_2^x \\ \vdots & \vdots & \cdots & \vdots \\ z_n^1 & z_n^2 & \cdots & z_n^x \end{pmatrix}, \tag{14}$$

where U*c* is the normalized eigenvectors of the U priority matrix.

$\forall z_b \in Z, \qquad b = 1, 2, \ldots . n$:

$$R_j = \begin{pmatrix} 1 & {r_1}/{r_2} & \ldots & {r_1}/{r_s} \\ {r_2}/{r_1} & 1 & \ldots & {r_2}/{r_s} \\ \vdots & \vdots & \ldots & \vdots \\ {r_s}/{r_1} & {r_s}/{r_2} & \ldots & 1 \end{pmatrix}, \tag{15}$$

where R*j* is the resource pair matrix.

$$R_c = \begin{pmatrix} r_1^1 & r_1^2 & \ldots & r_1^z \\ r_2^1 & r_2^2 & \ldots & r_2^z \\ \vdots & \vdots & \ldots & \vdots \\ r_s^1 & r_s^2 & \ldots & r_s^z \end{pmatrix}, \tag{16}$$

where R*c*-R is a matrix of normal vectors normalized to the predominant matrix.

$\forall r_v \in R, \qquad v = 1, 2, \ldots . s$:

$$A_i = \begin{pmatrix} 1 & {a_1}/{a_2} & \ldots & {a_1}/{a_k} \\ {a_2}/{a_1} & 1 & \ldots & {a_2}/{a_k} \\ \vdots & \vdots & \ldots & \vdots \\ {a_k}/{a_1} & {a_k}/{a_2} & \ldots & 1 \end{pmatrix}, \tag{17}$$

where A*i* is a pairwise comparison matrix of information views.

$$A_c = \begin{pmatrix} a_1^1 & a_1^2 & \ldots & a_1^s \\ a_2^1 & a_2^2 & \ldots & a_2^s \\ \vdots & \vdots & \ldots & \vdots \\ a_k^1 & a_k^2 & \ldots & a_k^s \end{pmatrix}, \tag{18}$$

where A*c*-A is a matrix of normalized special vectors of the dominance matrix.

$a_j \in A, \qquad j = 1, 2, \ldots . k$:

$$B = \begin{pmatrix} 1 & {b_1}/{b_2} & \ldots & {b_1}/{b_n} \\ {b_2}/{b_1} & 1 & \ldots & {b_2}/{b_n} \\ \vdots & \vdots & \ldots & \vdots \\ {b_n}/{b_1} & {b_n}/{b_2} & \ldots & 1 \end{pmatrix}, \tag{19}$$

where B is a pairwise comparison matrix of business processes on the value criterion.

$$\mathrm{B}_c = \begin{pmatrix} b_1^1 & b_1^2 & \ldots & b_1^k \\ b_2^1 & b_2^2 & \ldots & b_2^k \\ \vdots & \vdots & \ldots & \vdots \\ b_n^1 & b_n^2 & \ldots & b_n^k \end{pmatrix}, \tag{20}$$

where B*c*-B are the normal vectors of the dominance matrix.

$$\mathrm{D} = \begin{pmatrix} \sum_{j=1}^{z} t_1^c * z_j^c * r_1^c & \sum_{j=1}^{z} t_1^c * z_j^c * r_2^c & \ldots & \sum_{j=1}^{z} t_1^c * z_j^c * r_s^c \\ \sum_{j=1}^{z} t_2^c * z_j^c * r_1^c & \sum_{j=1}^{z} t_2^c * z_j^c * r_2^c & \ldots & \sum_{j=1}^{z} t_2^c * z_j^c * r_s^c \\ \vdots & \vdots & \ldots & \vdots \\ \sum_{j=1}^{z} t_x^c * z_j^c * r_1^c & \sum_{j=1}^{z} t_x^c * z_j^c * r_2^c & \ldots & \sum_{j=1}^{z} t_x^c * z_j^c * r_s^c \end{pmatrix} \tag{21}$$

The threat analysis procedure is based on two criteria: the frequency of the threat and the magnitude of the damage seen when the threats are realized. In this case, the criterion of "magnitude of damage" refers to the potential threat threatening [8-9].

Intelligent systems are now used in many information protection processes because the efficiency and reliability of these systems are considered to be much higher [10]. If neural networks are used in the development of the defense mechanism, a significant increase in the operating speed of the system can be achieved, and an increase in speed does not reduce the reliability of the system [11].

## Conclusion

In summary, the first step of the analysis is to construct a matrix comparing Ta threats according to the frequency criterion of occurrence. A vulnerability comparison matrix Zv is then constructed for each threat, with a priority vector Zc indicating the most probable path to realizing the threats. The matrix of the impact of information threats on resources is then assessed for the greatest loss corresponding to the established relationships. After this step, the threat risk can be calculated according to formula (21). Additional features of the threat and vulnerability model allow the company to assess the impact of this or that threat on individual business processes and the business processes of the whole enterprise, the appearance of information.

**References:**

1. Bekmuratov T.F. Mul'tiagentnaya gibridnaya nechetko-neyronnaya e`kspertnaya sistema informacionnoy bezopasnosti // Problemy' informatiki i e`nergetiki - 2013 - Vy'p. 3-4. S. 3-14.
2. Men'shih V. V., Spiridonova N. E. Ocenki vozmojnosti nesankcionirovannogo dostupa v informacionnuyu sistemu s pomosch"yu metoda analiza ierarhiy // Tehnika i bezopasnost' ob`ektov ugolovno-ispolnitel'noy sistemy' : sbornik materialov mejdunarodnoy nauchno-prakticheskoy konferencii. - Voronej, 2018. - S. 241-244.
3. Filippov V. V., Romanov M. S. Sravnitel'ny'y analiz sovremenny'h integrirovanny'h sistem bezopasnosti // Aktual'ny'e voprosy' e`kspluatacii sistem ohrannogo monitoringa i zasch'isch'enny'h telekommunikacionny'h sistem : sbornik materialov vserossiyskoy nauchno-prakticheskoy konferencii. - Voronej, 2018. - S. 87-88.
4. Romanov M. S., Grechany'y S. A. Zadacha razrabotki matematicheskih modeley optimal'noy territorial'no raspredelennoy sistemy' centralizovannogo nablyudeniya Rosgvardii // Vestnik Voronejskogo instituta MVD Rossii. - 2018. - № 2. - S. 94-101.
5. Kocy'nyak M.A., Ivanov D. A. Obespechenie bezopasnosti upravleniya robotizirovanny'h sistem ot vozdeystviya targetirovanny'h kiberneticheskih atak // Tezisy' dokladov XVI Vserossiyskoy nauchnoy konferencii «Neyrokomp'yutery' i ih primenenie» (Moskva, 13 marta 2018). M.: Izd vo FGBOU VO MGPPU, 2018. S. 108 A.
6. Saati T. L. Otnositel'noe izmerenie i ego obobsch'enie v prinyatii resheniy. Pochemu parny'e sravneniya yavlyayutsya klyuchevy'mi v matematike dlya izmereniya neosyazaemy'h faktorov // Cloud Of Science". 2016. T. 3. № 2. C. 171-262.
7. Matveev V.A., Morozov A.M., Bel'fer R.A. Ocenka urovnya riska ugrozy' bezopasnosti froda v seti VoIP po protokolu SIP // E`lektrosvyaz'. 2014. № 6. S. 35-38.
8. Bel'fer R.A., Kalyujny'y D.A., Tarasova D.V. Analiz zavisimosti urovnya riska ugroz bezopasnosti setey svyazi ot e`kspertny'h danny'h pri raschetah s ispol'zovaniem teorii nechetkih mnojestv // Voprosy' kiberbezopasnosti. 2014. № 1 (2). S. 61-67.
9. Solov'ev S.V., Mamuta V.V. Primenenie apparata neyrosetevy'h tehnologiy dlya opredeleniya aktual'ny'h ugroz bezopasnosti informacii informacionny'h sistem // Naukoemkie tehnologii v kosmicheskih issledovaniyah Zemli. 2016. №5 (8). S. 78-81.
10. Vasil'ev V.I. Intellektual'ny'e sistemy' zasch'ity' informacii. 2017 g.
11. Bekmuratov Tulkun Fayzievich, Botirov Fayzullajon Bakhtiyorovich, Haydarov Elshod Dilshod ugli, Electronic spam filtering based on neural networks, Chemical technology. Control and management, 2020, №3(93), p. 59-65.