N. V. Lysak, Cand. Sc. (Eng.), Ass. Prof.; J. V. Mironova, Cand. Sc. (Economics);

O. L. Rudkovska

METHODOLOGICAL APPROACH TO EVALUATION OF DATA PROTECTION AT ENTERPRISES

The paper considers the influence of the values of certain parameters on the data security state in general. As a result of the research, mathematical model of the enterprise data protection level evaluation has been developed using mathematical apparatus of fuzzy logic.

Key words: *data protection, mathematical model, fuzzy logic.*

Introduction

Protection of information resources is one of the priority tasks as to ensuring security of enterprises in Ukraine since transition to informational society has changed the status of information. At present information can be both the means for ensuring security and, at the same time, it could carry threat and danger. In the conditions of postindustrial society information has become a strategic resource of economic and scientific-technological progress. Therefore, data protection at enterprises requires sufficient theoretical-methodological base [1]. Investigation of the possibility to use mathematical tools for evaluation of data security at the enterprise is a very important task in current conditions of Ukrainian economy development.

Application of various methods for data protection at enterprises was considered by many scientists, and namely: by V. V. But, V. V. Mykytenko, O. V. Grebeniuk, M. O. Zhivko, O. A. Sorokivska, V. S. Tsimbaliuk, A. M. Chorna. However, substantiation of the necessity to use mathematical models and research methods has remained an unsolved problem in the data protection sphere. The existing methods are not always available and user-friendly, they require considerable material expenses.

The paper aims at the elaboration of methodological approach to enterprise data security level evaluation, which will be characterized by a simplified procedure of security identification due to application of the fuzzy logic apparatus.

Target of the research is the process of improving the system of evaluation of data security level at enterprises.

Presentation of the basic material

After long periods of reforms, crisis and post-crisis periods, modification of the enterprises functioning conditions is observed in the economy of Ukraine. As a result, there is a vital necessity for such data security provision, which would ensure information environment protection and efficiency of informational provision of the management process at the enterprise. Therefore, data protection is a component of general social-economic security of the enterprise.

To illustrate disputability of the key moments, let us present brief interpretations of the basic categories.

Data protection is a set of methods and means for ensuring integrity, availability and confidentiality (privacy) of information in the conditions of threats of natural and artificial character, realization of which could bring harm to data owners and users [2; 3].

Information is protected in order to support the following properties:

- Integrity – information protection against unsanctioned modification or deletion of its part;
- Availability – provision of protected access to information as well as of the possibility of its sanctioned usage from any place at any time;
- Confidentiality (privacy) – data protection from unsanctioned familiarization with it [4]. It is

rather complicated process as it requires consideration of all significant factors and establishing of correct functional dependencies. However, it is important to filter a great number of factors in order to avoid those, which are collinear, confronting, interdependent, mutually complementing or duplicative.

In order to evaluate information security, methods for determining cost-effectiveness of the data protection measures and methods for assessing damage, caused by the threat of hacker attacks, are often used. The method of fuzzy sets has become widespread. In this case expert estimation of the probability to overcome the data protection system, the probability of delivering information unit to a consumer is used as well as of the delivery time and hardware complexity. Sometimes such indicators as proportion of the information department workers in the total number of employees and proportion of expenses for ensuring information security in the total amount of expenditures are used.

Besides, some researchers consider the following indicators:

- information efficiency
- coefficient of provision with information
- information protection coefficient [4; 5].

The list of parameters of information protection level evaluation and their concretization degree are determined by the following methodological condition: the number of parameters to be evaluated should be rather limited in order to provide taking promt management decisions. Formation and grouping of the parameters is based on the analysis of a wide variety of economic and social problems. Therefore, the set of input factors should satisfy the conditions of completeness, efficiency and minimality. To satisfy the completeness criterion, such number of parameters must be determined, which would cover all the aspects of enterprise activities while exclusion at least one of them would not change the result. On the basis of the set, formed according to the completeness criterion, a group with minimal degree of achieving the result by the effectiveness criterion should be distinguished. In accordance with the minimality criterion, the number of parameters should be reduced by exclusion of those, which are inverse, interdependent, mutually complementing or duplicative.

On the basis of the analysis of foreign and home research [2 – 7], key factors determining data protection level at the enterprise have been identified. Functional relationship between information protection level and the factors that influence it could be presented in the form of structural-logic diagram. Thus, a structural-logic diagram of information protection at the enterprise has been elaborated (Fig. 1).

We propose a set of input parameters l_c ($c = \overline{1,C}$); a set of indicators that are calculated on the basis of evaluation parameters x_i ($i = \overline{1,n}$); a function of transformation of input parameters into evaluation indicators $F_1 : L \to X$; a set of functions, which serve as a basis for identifying efficiency level of the information security policy $F_2 = F(f_1,\ldots,f_i)$; a set of output parameters $E = (e_j), j = \overline{1,J}$.

Thus, mathematical model of such process will be given by

$$\begin{aligned} &L \xrightarrow{F_1} X \xrightarrow{F_2} E, \partial e\, L = (l_c), c = \overline{1,C}, X = (x_i), i = \overline{1,4}, E = (e_j), j = \overline{1,J} \\ &F_1 = f(x_{11}, x_{12}); F_2 = f(x_{21}, x_{22}); F_3 = f(x_{31},\ldots,x_{36}); F_4 = f(x_{41},\ldots,x_{43}) \end{aligned}. \quad (1)$$

On the basis of the set of X parameters x_i a set of transformation functions has been formed:

F_1 – function of the efficiency of technical support; F_2 – function of the efficiency of personnel component; F_3 – function of the data flows management efficiency; F_4 – function of the software efficiency.

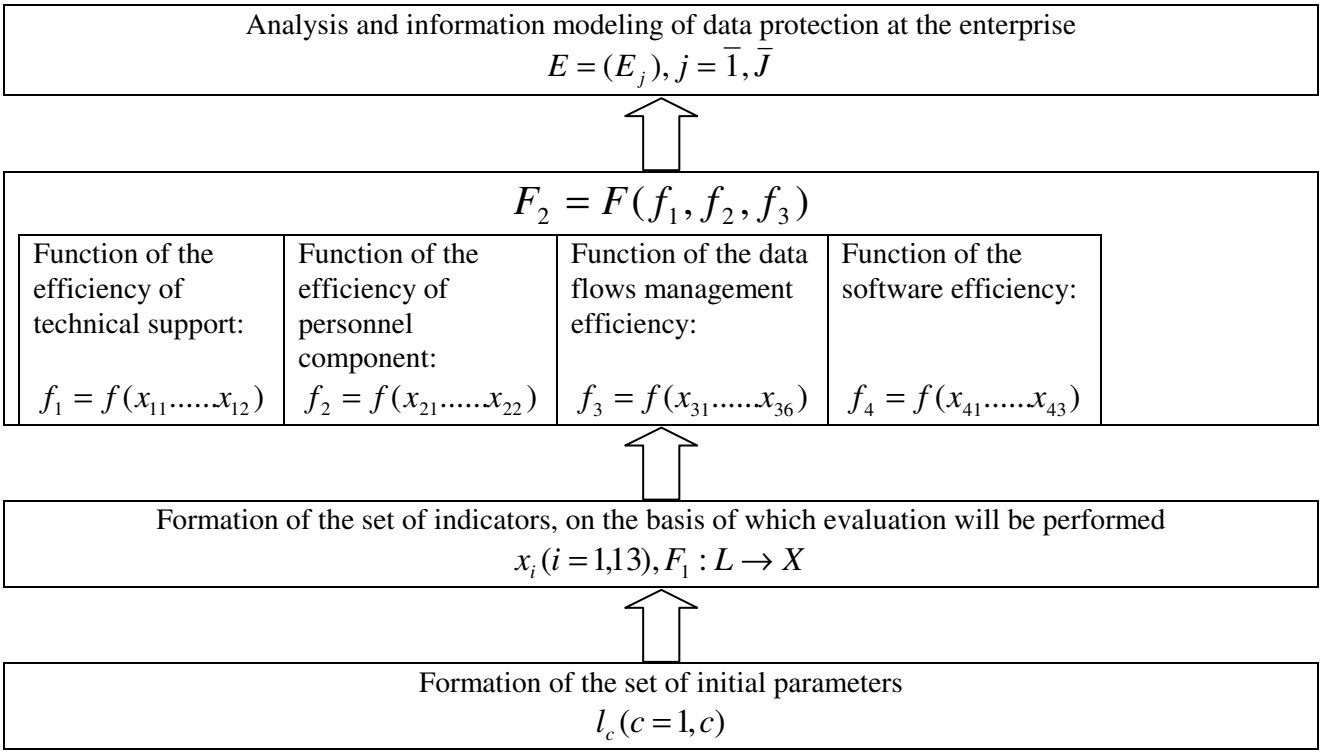

Fig. 1. Structural diagram of evaluation
of information protection level at the enterprise

As it was stated above, application of separate parameters (cost-effectiveness, data protection) and expert estimation methods does not enable efficient identification of information protection level at the enterprise. For efficient assessment of information protection at enterprises it is necessary to use modern mathematical tools which make it possible to combine not only indicators and models having different content, but also quantitative and qualitative parameters having different nature. The fuzzy logic apparatus is just such tool [8]. An important advantage of fuzzy models is their transparence, which enables their successful competition with various inductive methods of data processing [9].

Creation of the evaluation model includes 7 stages.

The first stage is determination of set T of linguistic terms, which consist from a set of linguistic variables. It should be noted that a variable is considered to be linguistic if it acquires its meaning from a list of words (word combinations) of natural or artificial language. For a set of three linguistic terms we have: L – low, A – average, H – high. For a set of 5 terms: L – low, BA – below average, A – average, AA – above average, H – high. Such quantity of linguistic terms takes into account the fact that the most accurate and adequate decisions are taken if 7 factors are analyzed.

In order to evaluate parameters (x_{11}, x_{12}, x_{21}, x_{22}, x_{31},…,x_{36}, x_{41},…,x_{43}) it is expedient to use three fuzzy terms since the parameters variation range is not very large. It should be noted that the parameters variation range is from 0 to 1 as standardization of the values was primarily performed. So, membership functions μ^{E_j}, j=$\overline{1, J}$ of three fuzzy terms were obtained. Taking into account expert opinions about specific nature of the selected parameters, the type of membership functions was chosen. Gaussian membership function, which most of all corresponds to the specificity of the chosen parameters, was used for all the parameters [8].

The aim of the second stage is determination of the graphs of membership functions. Graphs are determined for a set of parameters (x_{ij}). Membership function is determined for each linguistic term

separately on the basis of the existing list of membership functions [10 – 12].
General view of the membership function for different parameters is presented in Fig. 2, Fig. 3 and Fig. 4.

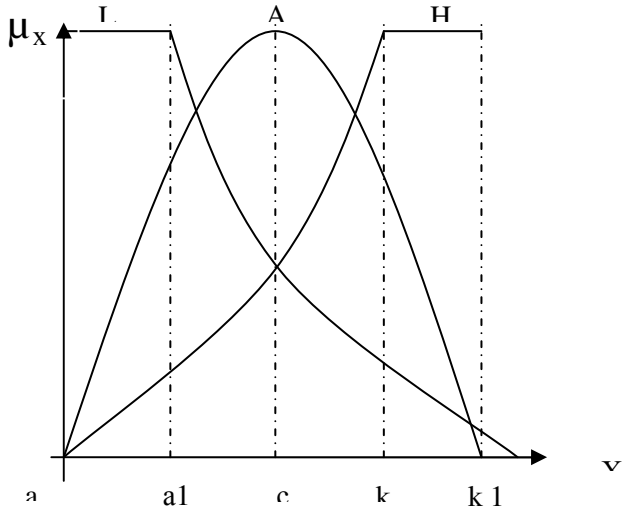

Fig. 2. General view of the membership function of three fuzzy terms for parameters x_{21}, x_{42}, x_{43}.

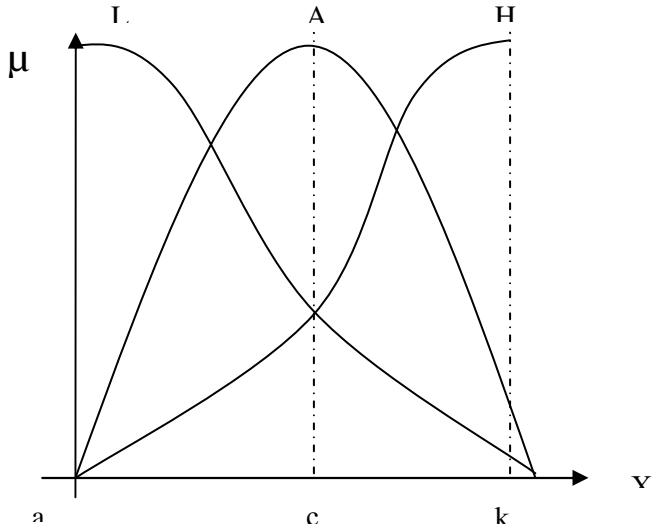

Fig. 3. General view of the membership function of three fuzzy terms for parameters x_{11}, x_{31}.

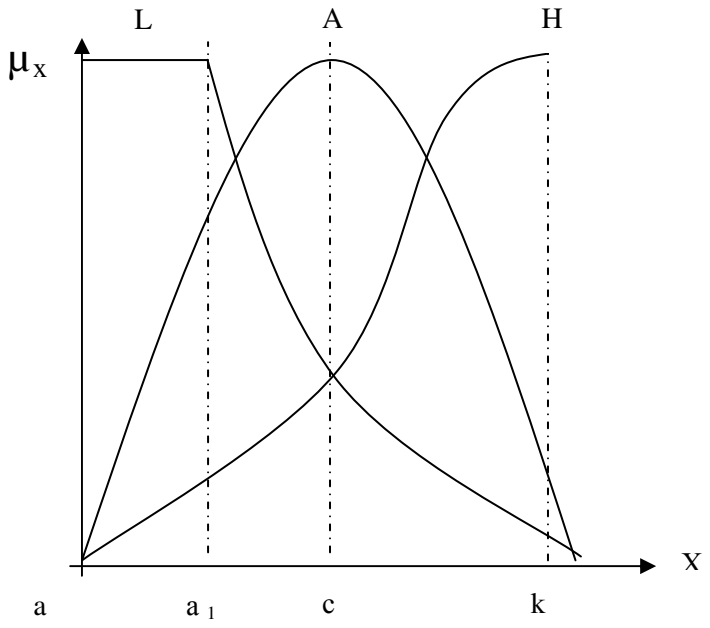

Fig. 4 general view of the membership function of three fuzy terms for parameters x_{12}, x_{22}, x_{32}, x_{33}, x_{34}, x_{35}, x_{36}, x_{41}.

Table 1

Input indicators of the model of enterprise data protection level evaluation

Abbreviated name of the indicator	Full name of the indicator
1. Efficiency of the enterprise technical support work	
X_{11}	information technical protection coefficent
X_{12}	the level of provision with technical means
2. Efficiency of the enterprise personnel component	
X_{21}	coefficient of the enterprise information service financing
X_{22}	personnel reliability coefficient
3. Efficiency of the enterprise data flows management	
X_{31}	information legal security coefficient
X_{32}	information completeness coefficient
X_{33}	information accuracy coefficient
X_{34}	information inconsistency coefficient
X_{35}	coefficient of timeliness of provision with information
X_{36}	information reliability coefficient
4. Enterprise software efficiency	
X_{41}	coefficient of the information protection with software
X_{42}	degree of provision with information protection software
X_{43}	software operation efficiency level

Explanations as to the chosen indicators and dependencies for their calculation are given below:
1) technical data protection coefficient (x_{11}):

$$K_{t.p.}=l_3/l_4, \quad (2)$$

where l_4 – a number of non-diverted information attacks.

2) the level of provision with technical means (x_{12}). It is calculated as a ratio between available technical means and those required.

3) coefficient of enterprise information service financing (x_{21}):

$$K_{fin} = \frac{l_1}{l_2}, \tag{3}$$

where l_1 – expenses for enterprise information services financing; l_2 – total expenses of the enterprise [3].

4) coefficient of reliability of the personnel ensuring enterprise information security (x_{22}):

$$K_{r.p} = \frac{l_7 - l_8}{l_7}, \tag{4}$$

where l_7 – total quantity of the dismissed employees; l_8 – number of employees dismissed because of information leakage

5) information legal security coefficient (x_{31}):

$$K_{leg.s} = \frac{l_5}{l_6}, \tag{5}$$

where l_5 – volume of information, leakage of which could cause negative consequences for the enterprise; l_6 – total volume of the legally protected information [5].

6) information completeness coefficient (x_{32}):

$$K_{com.inf.} = \frac{l_{10}}{l_9}, \tag{6}$$

where l_9 – volume of the available information, $l_{10.}$ – information volume required for taking a justified decision.

7) information accuracy coefficient (x_{33}):

$$K_{ac.inf.} = \frac{l_{11}}{l_{12}}, \tag{7}$$

where l_{11} – volume of the relevant information, l_{12} – volume of available information;

8) information inconsistency coefficient (x_{34}):

$$K_{inc.inf.} = \frac{l_{13}}{l_{14}}, \tag{8}$$

where l_{13} – number of independent evidences for taking decision, l_{14} – total number of independent evidences in the total volume of relevant information.

9) coefficient of timeliness of information provision (x_{35}):

$$K_{t.p.in.} = \frac{l_{15.}}{l_{16}}, \tag{9}$$

где $l_{15.}$ – volume of the timely provided information, l_{16} – volume of information necessary for taking a justified decision.

10) information reliability coefficient(x_{36}):

$$K_{r.in.} = \frac{l_{17}}{l_{18}}, \tag{10}$$

where l_{17} – volume of information provided from reliable sources, l_{18} – total volume of the provided information.

11) information software protection coefficient (x_{41}):

$$K_{s.p.} = \frac{l_{19}}{l_{20}}, \tag{11}$$

where l_{19} – time of smooth-running operation of the corporate information system, l_{20} – standard time of the corporate information system operation [6].

12) degree of provision with data protection software (x_{42}). It is calculated as a ratio between the amount of available software and the required software.

13) software operation efficiency level (x_{43}).

At the third stage we determine mathematical formulas, which describe preliminary selected membership functions μ^{E_j}, $j=\overline{1,J}$.

For the first membership function, shown in Fig. 2, mathematical formula has the form of:

$$\mu^{H}(x) = \begin{cases} 1, x \in [a; a_1) \\ \left(\dfrac{k-x}{k_1-a_1}\right)^n, x \in [a_1; k] \end{cases} \tag{12}$$

$$\mu^{C}(x) = \frac{1}{1+\left(\dfrac{x-c}{n}\right)^n} \tag{13}$$

$$\mu^{B}(x) = \begin{cases} \left(\dfrac{x-a}{k-a}\right)^n, x \in [a; k] \\ 1, x \in (k; k_1] \end{cases} \tag{14}$$

For the membership function of Fig. 3 mathematical formula is given by :

$$\mu^{H}(x)=\frac{1}{1+\left(\frac{k_1-x}{k_1-a}\right)^{n}} \tag{15}$$

$$\mu^{C}(x)=\frac{1}{1+\left(\frac{x-c}{n}\right)^{n}} \tag{16}$$

$$\mu^{B}(x)=\frac{1}{1+\left(\frac{x-k_1}{n}\right)^{n}} \tag{17}$$

For the membership function, presented in Fig. 4, mathematical formula has the form of:

$$\mu^{H}(x)=\begin{cases}1, x\in[a;a_1)\\ \left(\frac{k-x}{k_1-a_1}\right)^{n}, x\in[a_1;k]\end{cases} \tag{18}$$

$$\mu^{C}(x)=\frac{1}{1+\left(\frac{x-c}{n}\right)^{n}} \tag{19}$$

$$\mu^{B}(x)=\frac{1}{1+\left(\frac{x-k_1}{n}\right)^{n}} \tag{20}$$

At the next stage we form groups of indicators and establish numerical intervals for three terms (Table 2). Depending on the nature of economic phenomenon, we choose one of the three functions (graphs) for each parameter.

Table 2

Formulation of the indicators according to the scale of fuzzy terms "0 – 1"

Full name of the indicator	Abbreviated name of the indicator	Graph	Value of the indicators for the terms		
			L	A	H
I. Efficiency of the enterprise technical support work					
information technical protection coefficient	X_{11}	Fig. 3	0	0,2	1
the level of provision with technical means	X_{12}	Fig. 4	0- 0,2	0,5	1
II. Efficiency of the enterprise personnel component					
coefficient of the enterprise information service financing	X_{21}	Fig. 2	0- 0,3	0,5	0,7-1
personnel reliability coefficient	X_{22}	Fig. 4	0- 0,3	0,5	1
III. Efficiency of the enterprise data flows management					
information legal security coefficient	X_{31}	Fig. 3	0	0,5	1
information completeness coefficient	X_{32}	Fig. 4	0- 0,2	0,4	1
data accuracy coefficient	X_{33}	Fig. 4	0-0,2	0,4	0,6-1
information inconsistency coefficient	X_{34}	Fig. 4	0-0,1	0,5	1
coefficient of timeliness of provision with information	X_{35}	Fig. 4	0-0,1	0,5	1
information reliability coefficient	X_{36}	Fig. 4	0-0,1	0,5	1
IV. Efficiency of the enterprise software					
information software protection coefficient	X_{41}	Fig. 4	0-0,1	0,5	1
degree of provision with information protection software	X_{42}	Fig. 2	0- 0,3	0,5	0,6-1
level of the software operation efficiency	X_{43}	Fig. 2	0- 0,3	0,5	0,6-1

At he next stage of building the mathematical model of evaluating the efficiency of enterprise information protection policy, knowledge matrices for assessing the group of evaluation parameters were composed with the application of preliminary obtained information about the values of parameters. The composed matrices were described by logic equations establishing relation between f_i.

As a result, a methodological approach to information protection level evaluation at the domestic enterprises was elaborated, which enables essential reduction of expenses, caused by data losses, and ensures enterprise information space security. [13].

Conclusions

Investigation of the methodological tools for mathematical model elaboration has made it possible to obtain a complex mathematical model of information protection efficiency evaluation. This enables taking into account all the basic factors, which influence information protection level, and identifying weak points in the information security policy.

The developed mathematical model of the enterprise information protection level evaluation enables the assessment, which takes into account four groups of indicators reflecting the level of quantitative and qualitative aspects of information protection efficiency: at the level of technical protection, at the level of the work of personnel ensuring information security, at the level of data flows management and at the level of software component efficiency. The model consists from

logic equations describing the relations between the factors that influence information security level.

Following the presented recommendations, domestic enterprises would be able to maintain the proper information security level in accordance with current requirements.

REFERENCES

1. Сорокіна І. В. Теоретико-методологічні аспекти формування системи економічної безпеки підприємства / І. В. Сорокіна // Актуальні проблеми економіки. – 2009. – №12 (102). – С. 114 – 122.

2. Архипов А. Е. Технологии экспертного оценивания в задачах защиты информации / А. Е. Архипов, С. А. Архипова, С. А. Носок // Інформаційні технології та комп'ютерна інженерія : міжнар. наук.-техн. журн. – 2005. – № 1. – С. 89 – 94.

3. Степанов А. В. Характерные особенности задачи построения комплексной системы защиты информации распределенных корпоративных ресурсов / А. В. Степанов // Захист інформації. – 2007. – Спец. вип. – С. 131 – 134.

4. Дудикевич В. Б. Ієрархічна модель захисту даних в інформаційних технологіях / В. Б. Дудикевич, Г. В. Микитин, Ю. Р. Гарасим // Проблеми і перспективи Роозвитку ІТ-індустрії : зб. тез. доп. ІІ Міжнар. наук.-практ. конф. – Харків : Вид-во ХНУРЕ, 2010. – С. 212 – 213.

5. Ілляшенко С. М. Економічний ризик : навч. посіб. 2-ге вид., доп., перероб. / С. М. Ілляшенко. – К. : Центр навчальної літератури, 2004. – 220 с.

6. Реверчук Н. Й. Управління економічною безпекою підприємницьких структур : монографія / Н. Й. Реверчук. – Львів: ЛБІ НБУ, 2004. – 195 с.

7. Ермошин В. В. Методика оценки информационных рисков предприятия / В. В. Ермошин // Захист інформації. – 2009. – №4 (45). – С. 80 – 88.

8. Ротштейн А. П. Інтелектуальні технології ідентифікації: нечіткі множини, генетичні алгоритми, нейронні мережі : монографія / А. П. Ротштейн. – Вінниця : Універсум-Вінниця, 1999. – 320 с.

9. Штовба С. Д. Порівняння критеріїв навчання нечіткого класифікатора / С. Д. Штовба // Вісник ВПІ. – 2007. – № 6. – С. 84 – 91.

10. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А. Г. Корченко. – К. : "МК-Прес", 2006. – 320 с

11. Самарский А. А. Математическое моделирование : Идеи. Методы. Примеры / А. А. Самарский, А. П. Михайлов. – М. : Физматлит, 2001. – 213 с.

12. Сергеева Л. Н. Нелинейная экономика: модели и методы / Л. Н. Сергеева. – Запорожье : Полиграф, 2003. – 217 с.

13. Стасюк А. И. Анализ методов выполнения нечетких операций над нетолерантными числами для использования в системах защиты информации / А. И. Стасюк, А. Г. Корченко, В. В. Душеба, В. А. Рындюк, Н. В. Семенова // Зб. наук. пр. Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова. – 2002. – Вип. 18. – С. 27 – 30.

Lysak Nataliya **–** Cand. Sc. (Eng.), Ass. Prof. of the Department of Management and Security of Information Systems.

Mironova Juliya **–** Senior lecturer of the Department of Management and Security of Information Systems.

Rudkovska Olga **–** Junior lecturer of the Department of Finances.
Vinnytsia National Technical University.