Journal of Theoretical and Applied Information Technology
20th May 2016. Vol.87. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IMPROVED METHOD FOR THE FORMATION OF LINGUISTIC STANDARDS FOR OF INTRUSION DETECTION SYSTEMS

[1]AKHEMETOV BAKHYTZHAN , [2]KORCHENKO ANNA, [3]AKHMETOVA SANZIRA , [4]ZHUMANGALIEVA NAZYM

[1]Assoc Prof., Doctor of Technical , Institute of Information and Telecommunication Technologies, Kazakh National Technical University named after K. I. Satpayev, Almaty, Kazakhstan,

[2] Department of Information Technology Security, National Aviation University, Kyiv, Ukraine.
[3] Institute of Information and Telecommunication Technologies, Kazakh National Technical University named after K. I. Satpayev, Almaty, Kazakhstan,

[4] Institute of Information and Telecommunication Technologies, Kazakh National Technical University named after K. I. Satpayev, Almaty, Kazakhstan,

E-mail: [1]bakhytzhan.akhmetov.54@mail.ru, [2]annakor@ukr.net, [3]sanzira52@mail.ru, [4]nazym_k.81@mail.ru

ABSTRACT

Due to intensive development of digital business, malicious software and other cyber threats are becoming more common. To increase the level of security necessary special remedies that can be effective when new types of threats and allow fuzzy conditions to detect cyberattacks targeting multiple resources of information systems. Different attacking effects on related resources give rise to different sets of parametric anomalies in a heterogeneous environment. Known tuple model of the formation of a set of core components that allow to detect cyberattacks. For its effective application requires a formal approach to the formation of fuzzy (linguistic) standards. To this end a method is developed that focuses on the tasks of identifying cyberattacks on computer systems, which is based on mathematical models and methods of fuzzy logic and is implemented through six basic stages: the formation of subsets of identifiers linguistic assessments, forming the base matrix of frequencies, the formation of the derivative matrix of frequencies, the formation of fuzzy terms, the formation of the reference fuzzy numbers, visualization of linguistic standards. The method allows to improve the process of formalization of linguistic standards receive options to improve the efficiency of construction of the corresponding intrusion detection systems.
Keywords: *Artificial Neural Network (ANN), Static Var Compensator (SVC), Autonomous Hybrid Power System (AHPS)*

1. INTRODUCTION

1.1 Relevance

The formation of many markets and industries today it is difficult to imagine without information technologies. Due to the development of digital business and the Internet, malicious software and other cyber threats are becoming more prevalent and pervasive. In this regard, the necessary means to detect cyberattacks on various resources of information systems. For this purpose, special means of combating that is able to remain effective when new types of threats, characterized by unknown or vaguely defined criteria. It should be noted that such remedies can in fact remain functional formalized in fuzzy environment [1]. Apply required methods and models of information security based on fuzzy sets for building detection of anomalies generated by the corresponding offensive environment [2], is the basis for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

successful response to cyberattacks. Important in detecting anomalies, generated by cyberattacks, is the formation of fuzzy standards [2]. On this basis, the development of methods that improve the process of formalization of receiving linguistic standards of the parameters for the intrusion detection systems, there is actual scientific task.

1.2 Analysis Of Existing Research

A number of famous, quite effective developments used to solve these problems, detect cyberattacks, such as: the tuple model to form the basic component for the detection of cyberattacks [2], fuzzy approaches to intrusion detection [3]–[4] and detecting anomalies [5]; the corresponding fuzzy model [1], [6]–[7], methods [8]–[10] and intrusion detection system [11]–[13]; the sets of fuzzy rules [3]–[4], [8], [14]–[22], as well as other developments that are used for solving problems in fuzzy environment [23]. These studies demonstrated efficiency of application of mathematical apparatus of fuzzy sets, and its use to formalize the approach to identifying cyberattacks would improve the process of creating appropriate systems of detection of intrusions. It should be noted that many of the attacking effects on the resources of the information systems generate a lot of anomalies among the heterogeneous variables in a parametric environment [2].

For effective application of known models [2], [24] the formal implementation of the process of formation of fuzzy (linguistic) standards that will allow in a given linguistic variable identifies the search term [10]. On this term by using the corresponding sets of rules to determine the level of abnormal condition created by the impact of the corresponding class of cyberattacks.

1.3 Main Objective Of Research

Based on the analysis of existing research and the relevance of the task the aim of this work is to develop an improved (generalized) method of formation of linguistic standards (MFLS) for intrusion detection systems, operating in formalized fuzzy environment.

With such a method (when solving the tasks of identifying cyberattacks) can be formalized receiving process standards of the parameters for a given group of linguistic variables used to identify certain types of attacks on specific parametric heterogeneous environment in a specified time period.

2. MAIN PART OF RESEARCH

For construction of a subset of linguistic standards $\mathbf{T}_{ij}^{e}$ (see (13) in [2]), displaying the characteristic judgement of the expert concerning the anomalous state of the parameter P_{ij} we will develop an appropriate method that allows to formalize the process of obtaining standards of the parameters for the specified groups of linguistic variables for a specific environment. Improved method for the formation of linguistic standards (MFLS) is focused on solving the tasks of identifying cyberattacks on computer systems is a further development of the method of linguistic terms using statistical data [23] and is based on six stages.

Stage 1 – formation of subsets of identifiers linguistic assessments. The creation of the subset $\mathbf{LE}_{\mathbf{i}}$ is based on the set of all possible identifiers (ID) of linguistic evaluations (judgments) expert $\mathbf{LE}$ submitted as

$$\mathbf{LE} = \{\bigcup_{l=1}^{c} LE_l\} = \{LE_1, LE_2, \ldots, LE_c\}, (l = \overline{1,c}), \quad (1)$$

and that display used expert judgment to characterize the parameters $\mathbf{P_i}$ [2], [24] when observed in a m-dimensional parametric heterogeneous environment [2], and the c – number of such ID.

For example, when $c = 10$ according to (1) the set $\mathbf{LE}$ can be represented as follows:

$$\mathbf{LE} = \{\bigcup_{l=1}^{10} LE_l\} = \{LE_1, LE_2, \ldots, LE_{10}\} = \{LE_{VS}, LE_S, LE_A, LE_B, LE_{VB}, LE_Y, LE_M, LE_O, LE_L, LE_H\} = \{"VS", "S", "A", "B", "VB", "Y", "M", "O", "L", "H"\}, \quad (2)$$

where $LE_1 = LE_{VS} = "VS"$, $LE_2 = LE_S = "S"$, $LE_3 = LE_A = "A"$, $LE_4 = LE_B = "B"$, $LE_5 = LE_{VB} = "VB"$, $LE_6 = LE_Y = "Y"$, $LE_7 = LE_M = "M"$, $LE_8 = LE_O = "O"$, $LE_9 = LE_L = "L"$ and $LE_{10} = LE_H = "H"$ ID, respectively, are of such linguistic assessments (judgments) of expert as «VERY SMALL» (when $l = 1$), «SMALL» (when $l = 2$), «AVERAGE» (when $l = 3$), «BIG» (when $l = 4$), «VERY BIG» (when $l = 5$), «YOUTH» (when $l = 6$), «MEDIUM» (when $l = 7$), «OLD» (when

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$l=8$), «LOW» (when $l=9$) and «HIGH» (when $l=10$).

Next, we form the subset ID of expert judgments

$$\{\bigcup_{i=1}^{n}\mathbf{LE_i}\}=\{\mathbf{LE_1},\ \mathbf{LE_2},\ \ldots,\ \mathbf{LE_n}\}, \quad (3)$$

where $\mathbf{LE_i} \subseteq \mathbf{LE}$, $(i=\overline{1,n})$ defined as:

$$\mathbf{LE_i}=\{\bigcup_{j=1}^{m_i}\mathbf{LE_{ij}}\}=\{\mathbf{LE_{i1}},\mathbf{LE_{i2}},\ldots,\mathbf{LE_{im_i}}\}, \quad (4)$$

in this case $\mathbf{LE_{ij}}$ $(j=\overline{1,m_i})$ ID is a subset of the expert's judgments regarding the values of the parameters P_{ij} (see (8) в [2]) in m-dimensional parametric heterogeneous environment. Taking into consideration (4) we will write formula (3) in the following form:

$$\{\bigcup_{i=1}^{n}\mathbf{LE_i}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\mathbf{LE_{ij}}\}\}=\{\{\mathbf{LE_{11}},\ \mathbf{LE_{12}},\ \ldots,\ \mathbf{LE_{1m_1}}\},\ \{\mathbf{LE_{21}},\ \mathbf{LE_{22}},\ \ldots,\ \mathbf{LE_{2m_2}}\},\ \ldots,\ \{\mathbf{LE_{n1}},\ \mathbf{LE_{n2}},\ \ldots,\ \mathbf{LE_{nm_n}}\}\}. \quad (5)$$

Thus, taking into account $\mathbf{LE_{ij}} \subseteq \mathbf{LE_i}$, about j-th parameter the expert can apply a set from r_j statements (linguistic estimates), displayed by a subset

$$\mathbf{LE_{ij}}=\{\bigcup_{k=1}^{r_j}LE_{ijk}\}=\{LE_{ij1},LE_{ij2},\ldots,LE_{ijr_j}\}, \quad (6)$$

where LE_{ijk} $(k=\overline{1,r_j})$ – k-th identifier of a linguistic assessment of the expert concerning a state j-the parameter when i-th cyberattacks in a certain environment, but r_j – number of identifiers in LE_{ij}.

Further, the expression (5) with (6) takes the following form:

$$\{\bigcup_{i=1}^{n}\mathbf{LE_i}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\mathbf{LE_{ij}}\}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{k=1}^{r_j}LE_{ijk}\}\}\}=$$

$$\{\{\{LE_{111},\ LE_{112},\ \ldots,\ LE_{11r_1}\},\ \{LE_{121},\ LE_{122},\ \ldots,\ LE_{12r_2}\},\ \ldots,\ \{LE_{1m_11},\ LE_{1m_12},\ \ldots,\ LE_{1m_1r_{m_1}}\}\},\ \{\{LE_{211},\ LE_{212},\ \ldots,\ LE_{21r_1}\},\ \{LE_{221},\ LE_{222},\ \ldots,\ LE_{22r_2}\},\ \ldots,\ \{LE_{2m_21},\ LE_{2m_22},\ \ldots,\ LE_{2m_2r_{m_2}}\}\},\ \ldots,\ \{\{LE_{n11},\ LE_{n12},\ \ldots,\ LE_{n1r_1}\},\ \{LE_{n21},\ LE_{n22},\ \ldots,\ LE_{n2r_2}\},\ \ldots,\ \{LE_{nm_n1},\ LE_{nm_n2},\ \ldots,\ LE_{nm_nr_{m_n}}\}\}\}. \quad (7)$$

For example, when $n=3$ (i.e., to cyberattacks ID $CA_1=CA_{SN}=SN$ – «Scanning of ports (SN)», $CA_2=CA_{DS}=DS$ – «Denial of service (DS)» and $CA_3=CA_{SP}=SP$ – «Spoofing (SP)»), $m_1=m_3=2$, $m_2=3$, $r_1=5$, $r_2=r_3=3$ the expression (7) can be defined as:

$$\{\bigcup_{i=1}^{3}\mathbf{LE_i}\}=\{\bigcup_{i=1}^{3}\{\bigcup_{j=1}^{m_i}\mathbf{LE_{ij}}\}\}=\{\bigcup_{i=1}^{3}\{\bigcup_{j=1}^{m_i}\{\bigcup_{k=1}^{r_j}LE_{ijk}\}\}\}=$$

$$\{\{\{LE_{111},\ LE_{112},\ LE_{113},\ LE_{114},\ LE_{115}\},\ \{LE_{121},\ LE_{122},\ LE_{123}\}\},\ \{\{LE_{211},\ LE_{212},\ LE_{213},\ LE_{214},\ LE_{215}\},\ \{LE_{221},\ LE_{222},\ LE_{223}\},\ \{LE_{231},\ LE_{232},\ LE_{233}\}\},\ \{\{LE_{311},\ LE_{312},\ LE_{313},\ LE_{314},\ LE_{315}\},\ \{LE_{321},\ LE_{322},\ LE_{323}\}\}\}=$$

$$\{\{\{LE_{SNNVC1},\ LE_{SNNVC2},\ LE_{SNNVC3},\ LE_{SNNVC4},\ LE_{SNNVC5}\},\{LE_{SNVCA1},\ LE_{SNVCA2},\ LE_{SNVCA3}\}\},\ \{\{LE_{DSNCC1},\ LE_{DSNCC2},\ LE_{DSNCC3},\ LE_{DSNCC4},\ LE_{DSNCC5}\},\ \{LE_{DSSPR1},\ LE_{DSSPR2},\ LE_{DSSPR3}\},\ \{LE_{DSDBR1},\ LE_{DSDBR2},\ LE_{DSDBR3}\}\},\ \{\{LE_{SPNCC1},\ LE_{SPNCC2},\ LE_{SPNCC3},\ LE_{SPNCC4},\ LE_{SPNCC5}\},\ \{LE_{SPNPSA1},\ LE_{SPNPSA2},\ LE_{SPNPSA3}\}\}\}=$$

$$\{\{\{"VS", "S", "A", "B", "VB"\},\ \{"Y", "M", "O"\}\},\ \{\{"VS", "S", "A", "B", "VB"\},\ \{"L", "A", "H"\},\ \{"S", "A", "B"\}\},\ \{\{"VS", "S", "A", "B", "VB"\},\ \{"S", "A", "B"\}\}\},$$

where: $LE_{111}=LE_{SNNVC1}="VS"$, $LE_{112}=LE_{SNNVC2}="S"$, $LE_{113}=LE_{SNNVC3}="A"$, $LE_{114}=LE_{SNNVC4}="B"$, $LE_{115}=LE_{SNNVC5}=$ $"VB"$ and $LE_{121}=LE_{SNVCA1}="Y"$, $LE_{122}=$ $LE_{SNVCA2}="M"$,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$LE_{123} = LE_{SNVCA3} = "O"$ – ID, respectively, are such linguistic experts that show the status of settings $P_{11} = P_{SNNVC} = NVC$ «Numbers of Virtual channels» and $P_{12} = P_{SNVCA} = VCA$ «Virtual Channel Age» in 2-dimensional parametrical sub-environment [2];

$LE_{211} = LE_{DSNCC1} = "VS"$, $LE_{212} = LE_{DSNCC2} = "S"$, $LE_{213} = LE_{DSNCC3} = "A"$, $LE_{214} = LE_{DSNCC4} = "B"$, $LE_{215} = LE_{DSNCC5} = "VB"$, $LE_{221} = LE_{DSSPR1} = "L"$, $LE_{222} = LE_{DSSPR2} = "A"$, $LE_{223} = LE_{DSSPR3} = "H"$ and $LE_{231} = LE_{DSDBR1} = "S"$, $LE_{232} = LE_{DSDBR2} = "A"$, $LE_{233} = LE_{DSDBR3} = "B"$ – respectively the ID of linguistic experts, showing the status of parameters $P_{21} = P_{DSNCC} = NCC$ «Number of concurrent connections to the server», $P_{22} = P_{DSSPR} = SPR$ «Speed of processing requests from the clients» and $P_{23} = P_{DSDBR} = DBR$ «The delay between requests from the single user» in 3-dimensional parametrical sub-environment;

$LE_{311} = LE_{SPNCC1} = "VS"$, $LE_{312} = LE_{SPNCC2} = "S"$, $LE_{313} = LE_{SPNCC3} = "A"$, $LE_{314} = LE_{SPNCC4} = "B"$, $LE_{315} = LE_{SPNCC5} = "VB"$ and $LE_{321} = LE_{SPNPSA1} = "S"$, $LE_{322} = LE_{SPNPSA2} = "A"$, $LE_{323} = LE_{SPNPSA3} = "B"$ – ID, respectively, are such expert judgments that show the status of settings $P_{31} = P_{SPNCC} = NCC$ and $P_{32} = P_{SPNPSA} = NPSA$ «Number of packages with the same sender and receiver address» in 2-dimensional parametrical sub-environment.

It should be noted that the expert Express his opinions on the state of the observed actual values of various parameters in a particular environment, but it can use the same statements from the set of $\mathbf{LE}$, displayed appropriate language identifiers. For example, ID linguistic evaluation expert $"VS"$ for parameters $P_{11} = P_{SNNVC} = NVC$ ($LE_{111} = LE_{SNNVC1} = "VS"$) and $P_{21} = P_{DSNCC} = NCC$ ($LE_{211} = LE_{DSNCC1} = "VS"$) are merely linguistic equivalents of certain values of these quantities and, in fact, some characterize their relative condition, display the appropriate experts.

Stage 2 – formation of the basic matrix of frequencies. To obtain such matrix is filled in with the set of identifiers of the intervals $\mathbf{N}$ and a subset of these identifiers $\mathbf{N_i}$, which are displayed as

$$\{\bigcup_{i=1}^{n} \mathbf{N_i}\} = \{\mathbf{N_1}, \mathbf{N_2}, \ldots, \mathbf{N_n}\}, \quad (8)$$

where $\mathbf{N_i} \subseteq \mathbf{N}$, $(i = \overline{1,n})$ we will define as

$$\mathbf{N_i} = \{\bigcup_{j=1}^{m_i} \mathbf{N_{ij}}\} = \{\mathbf{N_{i1}}, \mathbf{N_{i2}}, \ldots, \mathbf{N_{im_i}}\}, \quad (9)$$

in this case $\mathbf{N_{ij}}$ $(j = \overline{1,m_i})$ – the ID subset of intervals, for determining which linguistic expert carries out the evaluation regarding the values of the parameters P_{ij} (see (8) in [2]) in m-dimensional parametric heterogeneous environment. Taking into account (9) we will write down formula (8) in the following form:

$$\{\bigcup_{i=1}^{n} \mathbf{N_i}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i} \mathbf{N_{ij}}\}\} = \{\{\mathbf{N_{11}}, \mathbf{N_{12}}, \ldots, \mathbf{N_{1m_1}}\}, \{\mathbf{N_{21}}, \mathbf{N_{22}}, \ldots, \mathbf{N_{2m_2}}\}, \ldots, \{\mathbf{N_{n1}}, \mathbf{N_{n2}}, \ldots, \mathbf{N_{nm_n}}\}\}. \quad (10)$$

Further, taking into account $\mathbf{N_{ij}} \subseteq \mathbf{N_i}$, about j-th parameter expert for forming the borders of their assessments may use the set of r_j intervals, the displayed subset

$$\mathbf{N_{ij}} = \{\bigcup_{k=1}^{r_j} N_{ijk}\} = \{N_{ij1}, N_{ij2}, \ldots, N_{ijr_j}\}, \quad (11)$$

where N_{ijk} $(k = \overline{1,r_j})$ – identifier of k-th interval used for the formation of frequencies of occurrence of experts on the current state j-th parameter relative i-th cyberattacks in a certain environment, but r_j – the number of IDs fixed intervals on which the assessment.

Then the expression (10) with (11) takes the following form:

$$\{\bigcup_{i=1}^{n} \mathbf{N_i}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i} \mathbf{N_{ij}}\}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{k=1}^{r_j} N_{ijk}\}\}\} = \{\{\{N_{111}, N_{112}, \ldots, N_{11r_1}\}, \{N_{121}, N_{122}, \ldots, N_{12r_2}\}, \ldots, \{N_{1m_1 1}, N_{1m_1 2}, \ldots, N_{1m_1 r_{m_1}}\}\}, \{\{N_{211}, N_{212}, \ldots, N_{21r_1}\}, \{N_{221}, N_{222}, \ldots, N_{22r_2}\}, \ldots, \{N_{2m_2 1}, N_{2m_2 2}, \ldots, N_{2m_2 r_{m_2}}\}\}, \ldots, \{\{N_{n11}, N_{n12}, \ldots, N_{n1r_1}\}, \{N_{n21}, N_{n22}, \ldots, N_{n2r_2}\}, \ldots, \{N_{nm_n 1}, N_{nm_n 2}, \ldots, N_{nm_n r_{m_n}}\}\}\}. \quad (12)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Based on the elements of the subsets $\mathbf{LE_{ij}}$ and $\mathbf{N_{ij}}$ formed synthesis table of assessments (table 1), the content of which is based on the current fixation evidence (judgments, evaluations), expert, where f_{ijsq} $(s,q=\overline{1,r_j})$ – elements of empirical data showing the number (frequency) of the same utterances (the use of linguistic assessments of the subset $\mathbf{LE_{ij}}$) expert, characterizing the state of the j-th parameter on the interval ID $N_{ijq} \overset{def}{=} [N_{ijq}^{min}; N_{ijq}^{max}]$ $(q=\overline{1,r_j})$, where N_{ijq}^{min} and N_{ijq}^{max} respectively the lower and upper bound q-th interval.

Table 1

Generalized table of assessments $\mathbf{LE_{ij}}$

	$\mathbf{N_{ij}}$					
		N_{ij2}	…		…	
		f_{ij12}	…		…	
		f_{ij22}	…		…	
		f_{ijs2}	…		…	
		f_{ijr_j2}	…		…	

Further on the basis of generalized evidence on the elements of the subset $\mathbf{LE_{ij}}$ (see table 1) formed the basic matrix of frequencies

$$F_{ij} = \left\| f_{ij} \begin{matrix} f_{ij12} & \dots & \dots \\ f_{ij22} & \dots & \dots \\ f_{ijs2} & \dots & \dots \\ f_{ijr_j2} & \dots & \dots \end{matrix} \right\| \qquad (13)$$

For example, if you want to build a matrix F_{ij} $(s,q=\overline{1,r_j})$, which will be the basis for building standards $\mathbf{T_{ij}^e}$, when $n=3$ (i.e. cyberattacks with ID $CA_1=CA_{SN}=SN$, $CA_2=CA_{DS}=DS$ and $CA_3=CA_{SP}=SP$), $m_1=m_3=2$, $m_2=3$, $r_1=5$, $r_2=r_3=3$ the expression (12) can be defined as:

$$\{\bigcup_{i=1}^{3}\mathbf{N_i}\}=\{\bigcup_{i=1}^{3}\{\bigcup_{j=1}^{\mathbf{m_i}}\mathbf{N_{ij}}\}\}=\{\bigcup_{i=1}^{3}\{\bigcup_{j=1}^{m_i}\{\bigcup_{k=1}^{r_j}N_{ijk}\}\}\}=$$
$$\{\{\{N_{111}, N_{112}, N_{113}, N_{114}, N_{115}\},$$
$$\{N_{121}, N_{122}, N_{123}\}\},$$
$$\{\{N_{211}, N_{212}, N_{213}, N_{214}, N_{215}\},$$
$$\{N_{221}, N_{222}, N_{223}\}, \{N_{231}, N_{232}, N_{233}\}\},$$
$$\{\{N_{311}, N_{312}, N_{313}, N_{314}, N_{315}\},$$
$$\{N_{321}, N_{322}, N_{323}\}\}\}=$$
$$\{\{\{N_{SNNVC1}, N_{SNNVC2}, N_{SNNVC3}, N_{SNNVC4},$$
$$N_{SNNVC5}\}, \{N_{SNVCA1}, N_{SNVCA2}, N_{SNVCA3}\}\},$$
$$\{\{N_{DSNCC1}, N_{DSNCC2}, N_{DSNCC3}, N_{DSNCC4},$$
$$N_{DSNCC5}\}, \{N_{DSSPR1}, N_{DSSPR2}, N_{DSSPR3}\},$$
$$\{N_{DSDBR1}, N_{DSDBR2}, N_{DSDBR3}\}\},$$
$$\{\{N_{SPNCC1}, N_{SPNCC2}, N_{SPNCC3},$$
$$N_{SPNCC4}, N_{SPNCC5}\},$$
$$\{N_{SPNPSA1}, N_{SPNPSA2}, N_{SPNPSA3}\}\}\}. \qquad (14)$$

For example, according to (14) when $n=1$, ($i=3$ i.e., to cyberattacks with ID $CA_3=CA_{SP}=SP$), $j=2$, $r_j=3$ для $\{N_{321}, N_{322}, N_{323}\}$ on the basis of the generalized tables (see table 1) build the current table of assessments (table 2) on the elements of the subset $LE_{ijk}=LE_{32k}=LE_{SPNPSAk}$ $(r_2=3,\ k=\overline{1,3})$, where $LE_{321}=LE_{SPNPSA1}="S"$, $LE_{322}=LE_{SPNPSA2}="A"$, $LE_{323}=LE_{SPNPSA3}="B"$ and $N_{ijk}=N_{32k}=N_{SPNPSAk}$, but $N_{ij1}=N_{321}=N_{SPNPSA1} \overset{def}{=} [N_{SPNPSA1}^{min}; N_{SPNPSA1}^{max}] <=> [0; 10]$, $N_{ij2}=N_{322}=N_{SPNPSA2} \overset{def}{=} [N_{SPNPSA2}^{min}; N_{SPNPSA2}^{max}] <=> [11; 100]$, $N_{ij3}=N_{323}=N_{SPNPSA3} \overset{def}{=} [N_{SPNPSA3}^{min}; N_{SPNPSA3}^{max}] <=> [101; 1000]$.

Table 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The current table estimates for $\mathbf{LE_{32}}$

$\mathbf{LE_{32}} =$ $\mathbf{LE_{S}}$	$\mathbf{N_{32}} = \mathbf{N_{SPNPSA}}$		
	N_{S}	N_{SP}	N_{SI}
$"S"$	3	1	0
$"A'$	1	4	2
$"B'$	0	2	3

Then, when $s,q=\overline{1,3}$ according to expression (13) using the data of table 2, we generate the matrix of frequencies, i.e.

$$F_{32}=F_{SPNPSA}=\left\|f_{32sq}\right\|=\left\|f_{SPNPSAsq}\right\|=$$

$$\left\|\begin{matrix} \cdot & f_{3212} & f_{3213} \\ \cdot & f_{3222} & f_{3223} \\ \cdot & f_{3232} & f_{3233} \end{matrix}\right\| = \left\| \quad \right\|$$

Stage 3 – formation of the derivative matrix of frequencies. To implement this step, you create a vector of sums (VS_{ij}) the appropriate columns of the frequency matrix of (13), i.e.

$$VS_{ij}=\left\|vs_{ijq}\right\|=\left\|vs_{ij1},vs_{ij2},\ldots,vs_{ijq},\ldots,vs_{ijr_j}\right\|=$$

$$\left\|\sum_{s=1}^{r_j}f_{ijs1},\sum_{s=1}^{r_j}f_{ijs2},\ldots,\sum_{s=1}^{r_j}f_{ijsq},\ldots,\sum_{s=1}^{r_j}f_{ijsr_j}\right\|=$$

$$\left\|\bigcup_{q=1}^{r_j}\sum_{s=1}^{r_j}f_{ijsq}\right\|,\ (s,q=\overline{1,r_j}), \qquad (15)$$

where f_{ijsq} – are the elements of the matrix F_{ij}. Further by the member of VS_{ij} defined a maximum value according to the formula

$$vsm_{ij}=\bigvee_{q=1}^{r_j}vs_{ijq}\ , \qquad (16)$$

which is used to form the derivative matrix of frequencies

$$F'_{ij}=\left\|f'_{ijsq}\right\|=(vsm_{ij}/vs_{ijq})\left\|f_{ijsq}\right\| \Longleftrightarrow$$

$$F'_{ij}=(vsm_{ij}/vs_{ijq})F_{ij}=$$

$$\left\|\begin{matrix} f'_{ij12} & \ldots & \ldots \\ f'_{ij22} & \ldots & \ldots \\ f'_{ijs2} & \ldots & \ldots \\ f'_{ijr_j2} & \ldots & \ldots \end{matrix}\right\|. \qquad (17)$$

Consider the formation of F'_{ij} on a concrete example. To do this, when $i=3$, $j=2$ we will create a vector of sums $VS_{ij}=VS_{32}$ the appropriate columns of the frequency matrix of (13) using expression (15), i.e.

$$VS_{32}=\left\|vs_{32q}\right\|=\left\|vs_{321},vs_{322},vs_{323}\right\|=$$

$$\left\|\bigcup_{q=1}^{3}\sum_{s=1}^{3}f_{32sq}\right\| \Longleftrightarrow VS_{SPNPSA}=\left\|vs_{SPNPSAq}\right\|=$$

$$\left\|vs_{SPNPSA1},vs_{SPNPSA2},vs_{SPNPSA3}\right\|=$$

$$\left\|\bigcup_{q=1}^{3}\sum_{s=1}^{3}f_{SPNPSAsq}\right\|=\left\|4,7,5\right\|,\ (q=\overline{1,3}).$$

Then from $VS_{32}=VS_{SPNPSA}$ by the formula (16) we will define a maximum element

$$vsm_{32}=\bigvee_{q=1}^{3}vs_{32q}=vs_{321}\vee vs_{322}\vee vs_{323}=$$

$$4\vee 7\vee 5=vsm_{SPNPSA}=7,$$

and the derivative matrix of frequencies

$$F'_{32}=\left\|f'_{32sq}\right\|=(vsm_{32}/vs_{32q})\left\|f_{32sq}\right\|=F'_{SPNPSA}$$

we will get according to the expression (17)

$$F'_{SPNPSA}=(vsm_{SPNPSA}/vs_{SPNPSAq})F_{SPNPSA}=$$

$$\left\|\begin{matrix} 5{,}3 & 1 & 0 \\ 1{,}8 & 4 & 2{,}8 \\ 0 & 2 & 4{,}2 \end{matrix}\right\|.$$

Stage 4 – formation of fuzzy terms. The construction of subsets of the fuzzy terms $\mathbf{T_i}$ is based on the set of all possible terms $\mathbf{T}$, showing the specific status of the corresponding parameters from $\mathbf{P_i}$ in m_i-dimensional parametrical sub-environment [2], i.e.

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{T_i}\}=\{\mathbf{T_1},\mathbf{T_2},\ldots,\mathbf{T_n}\}, \qquad (18)$$

where $\mathbf{T_i}\subseteq\mathbf{T}$, $(i=\overline{1,n})$, and

$$\mathbf{T_i}=\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{T_{ij}}\}=\{\mathbf{T_{i1}},\mathbf{T_{i2}},\ldots,\mathbf{T_{im_i}}\}, \qquad (19)$$

Journal of Theoretical and Applied Information Technology
20th May 2016. Vol.87. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

thus $\mathbf{T_{ij}}$ $(j=\overline{1,m_i})$ is a fuzzy subset of terms relative to the values of the parameters is a fuzzy subset of terms relative to the values of the parameters P_{ij} (see (8) in [2]). Taking into account (19) formula (18) we will write in the following form:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{T_i}\}=\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{T_{ij}}\}\}=$$

$$\{\{\mathbf{T_{11}},\ \mathbf{T_{12}},\ldots,\ \mathbf{T_{1m_1}}\},\ \{\mathbf{T_{21}},\ \mathbf{T_{22}},\ldots,\ \mathbf{T_{2m_2}}\},$$

$$\ldots,\ \{\mathbf{T_{n1}},\ \mathbf{T_{n2}},\ldots,\ \mathbf{T_{nm_n}}\}\},\ (j=\overline{1,m_i}).\quad(20)$$

Thus, taking into account $\mathbf{T_{ij}}\subseteq\mathbf{T_i}$ and (20), a subset of the fuzzy terms defined as:

$$\mathbf{T_{ij}}=\{\bigcup_{s=1}^{r_j}\underset{\sim}{T}_{ijs}\}=\{\underset{\sim}{T}_{ij1},\ \underset{\sim}{T}_{ij2},\ldots,\ \underset{\sim}{T}_{ijr_j}\},\quad(21)$$

where $\underset{\sim}{T}_{ijs}$ $(s=\overline{1,r_j})$ – are fuzzy terms, and r_j – the number of members in $\mathbf{T_{ij}}$.

Further, the expression (20) with (21) takes the following form:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{T_i}\}=\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{T_{ij}}\}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{r_j}\underset{\sim}{T}_{ijs}\}\}\}=$$

$$\{\{\{\underset{\sim}{T}_{111},\ \underset{\sim}{T}_{112},\ldots,\ \underset{\sim}{T}_{11r_1}\},\ \{\underset{\sim}{T}_{121},\ \underset{\sim}{T}_{122},\ldots,$$

$$\underset{\sim}{T}_{12r_2}\},\ldots,\ \{\underset{\sim}{T}_{1m_11},\ \underset{\sim}{T}_{1m_12},\ldots,\ \underset{\sim}{T}_{1m_1r_{m_1}}\}\},\ \{\{\underset{\sim}{T}_{211},$$

$$\underset{\sim}{T}_{212},\ldots,\ \underset{\sim}{T}_{21r_1}\},\ \{\underset{\sim}{T}_{221},\ \underset{\sim}{T}_{222},\ldots,\ \underset{\sim}{T}_{22r_2}\},\ldots,$$

$$\{\underset{\sim}{T}_{2m_21},\ \underset{\sim}{T}_{2m_22},\ldots,\ \underset{\sim}{T}_{2m_2r_{m_2}}\}\},\ldots,\ \{\{\underset{\sim}{T}_{n11},\ \underset{\sim}{T}_{n12},$$

$$\ldots,\ \underset{\sim}{T}_{n1r_1}\},\ \{\underset{\sim}{T}_{n21},\ \underset{\sim}{T}_{n22},\ldots,\ \underset{\sim}{T}_{n2r_2}\},\ldots,\ \{\underset{\sim}{T}_{nm_n1},$$

$$\underset{\sim}{T}_{nm_n2},\ldots,\ \underset{\sim}{T}_{nm_nr_{m_n}}\}\}\}.\ (22)$$

Next, it needs to generate the values displayed in the component $\underset{\sim}{T}_{ijs}$, what for the following transformations are used. On $F_{ij}^{'}$ matrix elements according to expression (23) the vector of maxima is under construction

$$FM_{ij}=\left\|fm_{ijq}\right\|=$$

$$\left\|fm_{ij1},fm_{ij2},\ldots,fm_{ijq},\ldots,fm_{ijr_j}\right\|=$$

$$\left\|\bigvee_{s=1}^{r_j}f_{ijs1}^{'},\bigvee_{s=1}^{r_j}f_{ijs2}^{'},\ldots,\ \bigvee_{s=1}^{r_j}f_{ijsq}^{'},\ldots,\ \bigvee_{s=1}^{r_j}f_{ijsr_j}^{'}\right\|=$$

$$\left\|\bigcup_{q=1}^{r_j}\bigvee_{s=1}^{r_j}f_{ijsq}^{'}\right\|,\ (s,q=\overline{1,r_j}).\qquad(23)$$

Based on FM_{ij} we generate the matrix of membership functions

$$M_{ij}=\left\|\mu_{ijsq}\right\|=$$

$$\left\|\begin{matrix}\mu_{ij12} & \ldots & \ldots\\ \mu_{ij22} & \ldots & \ldots\\ \mu_{ijs2} & \ldots & \ldots\\ \mu_{ijr_j2} & \ldots & \ldots\end{matrix}\right\|,\ (24)$$

each element of which is given by the expression $\mu_{ijsq}=f_{ijsq}^{'}/fm_{ijs}$ $(s,q=\overline{1,r_j})$. Using (24), we define the fuzzy sets of terms (numbers) $\underset{\sim}{T}_{ijs}$ on the basis of the expression

$$\underset{\sim}{T}_{ijs}=\{\bigcup_{q=1}^{r_j}\mu_{ijsq}\ /\ x_{ijsq}\}=\{\ \mu_{ijs1}\ /\ x_{ijs1},$$

$$\mu_{ijs2}\ /\ x_{ijs2},\ldots,\ \mu_{ijsr_j}\ /\ x_{ijsr_j}\},\ (q=\overline{1,r_j}),\ (25)$$

where

$$x_{ijsq}=N_{ijq}^{max}/N_{ijr_j}^{max}\ \ (q=\overline{1,r_j}).\qquad(26)$$

Note that the fuzzy number (FN) $\underset{\sim}{T}_{ijs}$ $(s=\overline{1,r_j})$ accordingly interpreting linguistic utterances of experts LE_{ijk} $(k=\overline{1,r_j})$, the display elements of the subset $\mathbf{LE_{ij}}\subseteq\mathbf{LE}$ (see (7)).

Show the process of formation $\mathbf{T_{ij}}$ of a specific example, when $n=3$ (i.e. for cyberattacks ID CA_1 $=CA_{SN}=SN$, $CA_2=$ $CA_{DS}=DS$ and $CA_3=CA_{SP}$ $=SP$), $m_1=m_3=$ 2, $m_2=3$, $r_1=5$, $r_2=r_3=3$ the expression (22) can be defined as:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{3}}\mathbf{T_i}\}=\{\bigcup_{\mathbf{i=1}}^{\mathbf{3}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{T_{ij}}\}\}=\{\bigcup_{i=1}^{3}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{r_j}\underset{\sim}{T}_{ijs}\}\}\}=$$

$$\{\{\{\underset{\sim}{T}_{111},\ \underset{\sim}{T}_{112},\ \underset{\sim}{T}_{113},\ \underset{\sim}{T}_{114},\ \underset{\sim}{T}_{115}\},$$

$$\{\underset{\sim}{T}_{121},\ \underset{\sim}{T}_{122},\ \underset{\sim}{T}_{123}\}\},$$

$$\{\{\underset{\sim}{T}_{211},\ \underset{\sim}{T}_{212},\ \underset{\sim}{T}_{213},\ \underset{\sim}{T}_{214},\ \underset{\sim}{T}_{215}\},$$

$$\{\underset{\sim}{T}_{221},\ \underset{\sim}{T}_{222},\ \underset{\sim}{T}_{223}\},\ \{\underset{\sim}{T}_{231},\ \underset{\sim}{T}_{232},\ \underset{\sim}{T}_{233}\}\},$$

$$\{\{\underset{\sim}{T}_{311},\ \underset{\sim}{T}_{312},\ \underset{\sim}{T}_{313},\ \underset{\sim}{T}_{314},\ \underset{\sim}{T}_{315}\},$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$\{\underset{\sim}{T}_{321},\ \underset{\sim}{T}_{322},\ \underset{\sim}{T}_{323}\}\}\}=$$
$$\{\{\{\underset{\sim}{VS}_{11},\ \underset{\sim}{S}_{11},\ \underset{\sim}{A}_{11},\ \underset{\sim}{B}_{11},\ \underset{\sim}{VB}_{11}\},$$
$$\{\underset{\sim}{Y}_{12},\ \underset{\sim}{M}_{12},\ \underset{\sim}{O}_{12}\}\},$$
$$\{\{\underset{\sim}{VS}_{21},\ \underset{\sim}{S}_{21},\ \underset{\sim}{A}_{21},\ \underset{\sim}{B}_{21},\ \underset{\sim}{VB}_{21}\},$$
$$\{\underset{\sim}{L}_{22},\ \underset{\sim}{A}_{22},\ \underset{\sim}{H}_{22}\},\ \{\underset{\sim}{S}_{23},\ \underset{\sim}{A}_{23},\ \underset{\sim}{B}_{23}\}\},$$
$$\{\{\underset{\sim}{VS}_{31},\ \underset{\sim}{S}_{31},\ \underset{\sim}{A}_{31},\ \underset{\sim}{B}_{31},\ \underset{\sim}{VB}_{31}\},$$
$$\{\underset{\sim}{S}_{32},\ \underset{\sim}{A}_{32},\ \underset{\sim}{B}_{32}\}\}\}=$$
$$\{\{\{\underset{\sim}{T}_{SNNVC1},\ \underset{\sim}{T}_{SNNVC2},\ \underset{\sim}{T}_{SNNVC3},\ \underset{\sim}{T}_{SNNVC4},$$
$$\underset{\sim}{T}_{SNNVC5}\},\ \{\underset{\sim}{T}_{SNVCA1},\ \underset{\sim}{T}_{SNVCA2},\ \underset{\sim}{T}_{SNVCA3}\}\},$$
$$\{\{\underset{\sim}{T}_{DSNCC1},\ \underset{\sim}{T}_{DSNCC2},\ \underset{\sim}{T}_{DSNCC3},\ \underset{\sim}{T}_{DSNCC4},$$
$$\underset{\sim}{T}_{DSNCC5}\},\ \{\underset{\sim}{T}_{DSSPR1},\ \underset{\sim}{T}_{DSSPR2},\ \underset{\sim}{T}_{DSSPR3}\},$$
$$\{\underset{\sim}{T}_{DSDBR1},\ \underset{\sim}{T}_{DSDBR2},\ \underset{\sim}{T}_{DSDBR3}\}\},$$
$$\{\{\underset{\sim}{T}_{SPNCC1},\ \underset{\sim}{T}_{SPNCC2},\ \underset{\sim}{T}_{SPNCC3},\ \underset{\sim}{T}_{SPNCC4},$$
$$\underset{\sim}{T}_{SPNCC5}\},\ \{\underset{\sim}{T}_{SPNPSA1},\ \underset{\sim}{T}_{SPNPSA2},\ \underset{\sim}{T}_{SPNPSA3}\}\}\}=$$
$$\{\{\{\underset{\sim}{VS}_{SNNVC},\ \underset{\sim}{S}_{SNNVC},\ \underset{\sim}{A}_{SNNVC},\ \underset{\sim}{B}_{SNNVC},$$
$$\underset{\sim}{VB}_{SNNVC}\},\ \{\underset{\sim}{Y}_{SNVCA},\ \underset{\sim}{M}_{SNVCA},\ \underset{\sim}{O}_{SNVCA}\}\},$$
$$\{\{\underset{\sim}{VS}_{DSNCC},\ \underset{\sim}{S}_{DSNCC},\ \underset{\sim}{A}_{DSNCC},\ \underset{\sim}{B}_{DSNCC},$$
$$\underset{\sim}{VB}_{DSNCC}\},\ \{\underset{\sim}{L}_{DSSPR},\ \underset{\sim}{A}_{DSSPR},\ \underset{\sim}{H}_{DSSPR}\},\ \{\underset{\sim}{S}_{DSDBR},$$
$$\underset{\sim}{A}_{DSDBR},\ \underset{\sim}{B}_{DSDBR}\}\},$$
$$\{\{\underset{\sim}{VS}_{SPNCC},\ \underset{\sim}{S}_{SPNCC},\ \underset{\sim}{A}_{SPNCC},$$
$$\underset{\sim}{B}_{SPNCC},\ \underset{\sim}{VB}_{SPNCC}\},$$
$$\{\underset{\sim}{S}_{SPNPSA},\ \underset{\sim}{A}_{SPNPSA},\ \underset{\sim}{B}_{SPNPSA}\}\}\}. \quad (27)$$

According to (27) when $i=3$, $j=2$, $r_j=3$ for $\{\underset{\sim}{T}_{321},\ \underset{\sim}{T}_{322},\ \underset{\sim}{T}_{323}\}$ we will form $\mathbf{T_{32}} \subseteq \mathbf{T}$, i.e.:

$$\mathbf{T_{32}}=\{\bigcup_{s=1}^{3}\underset{\sim}{T}_{32s}\}=\{\underset{\sim}{T}_{321},\ \underset{\sim}{T}_{322},\ \underset{\sim}{T}_{323}\}=$$
$$\{\underset{\sim}{T}_{SPNPSA1},\ \underset{\sim}{T}_{SPNPSA2},\ \underset{\sim}{T}_{SPNPSA3}\}=$$
$$\{\underset{\sim}{S}_{32},\ \underset{\sim}{A}_{32},\ \underset{\sim}{B}_{32}\},\ (s=\overline{1,3}),$$

where $\underset{\sim}{T}_{321}=\underset{\sim}{T}_{SPNPSA1}=\underset{\sim}{S}_{32}$, $\underset{\sim}{T}_{322}=\underset{\sim}{T}_{SPNPSA2}=\underset{\sim}{A}_{32}$ and $\underset{\sim}{T}_{323}=\underset{\sim}{T}_{SPNPSA3}=\underset{\sim}{B}_{32}$ respectively are FN $\underset{\sim}{S}_{32}$, $\underset{\sim}{A}_{32}$ and $\underset{\sim}{B}_{32}$, interpreting statements of the expert that are displayed by $LE_{SPNPSA1}="S"$, $LE_{SPNPSA2}="A"$ and $LE_{SPNPSA3}="B"$.

Further on the basis of expression (23) construct the vector of maxima on the respective lines $F'_{32}=F'_{SPNPSA}$ i.e.

$$FM_{SPNPSA}=\left\|fm_{SPNPSAs}\right\|=$$
$$\left\|fm_{SPNPSA1}, fm_{SPNPSA2}, fm_{SPNPSA3}\right\|=$$
$$\left\|5,3;\ 4;\ 4,2\right\|.$$

Based on FM_{SPNPSA} by the expression (24) we will form a matrix of membership functions M_{SPNPSA} thus obtaining:

$$M_{SPNPSA}=\left\|\mu_{SPNPSA\,sq}\right\|=\begin{Vmatrix} 1 & 0,2 & 0 \\ 0,5 & 1 & 0,7 \\ 0 & 0,5 & 1 \end{Vmatrix},$$

where $\mu_{SPNPSAsq}=f'_{SPNPSAsq}/fm_{SPNPSAs}$. On the basis of the calculated according to the expression (24) $\mu_{SPNPSAsq}$ $(s,q=\overline{1,3})$ and to the expression (26) $x_{SPNPSAsq}$ we will define sets of fuzzy terms $\underset{\sim}{T}_{SPNPSA}$ by the formula (25), i.e.

$$\underset{\sim}{T}_{32s}=\{\mu_{32s1}/x_{32s1},\ \mu_{32s2}/x_{32s2},\ \mu_{32s3}/x_{32s3}\}$$
$$\Leftrightarrow\ \underset{\sim}{T}_{SPNPSAs}=\{\mu_{SPNPSAs1}/x_{SPNPSAs1},$$
$$\mu_{SPNPSAs2}/x_{SPNPSAs2},\ \mu_{SPNPSAs3}/x_{SPNPSAs3}\},$$
$$(s=\overline{1,3}),$$

where according to the expression (26) $x_{SPNPSAsq}=N^{max}_{SPNPSAq}/N^{max}_{SPNPSAr_j}$, $(q=\overline{1,3})$ or $\{\bigcup_{q=1}^{3}x_{SPNPSAsq}\}=\{0,01;\ 0,1;\ 1\}$.

Thus, these members of the subset $\mathbf{T_{32}}$ (numeric form) are respectively display the members of the subset $\mathbf{LE_{32}}$ (7) (linguistic form) and are presented in the following form:

$$\underset{\sim}{T}_{321}=\underset{\sim}{T}_{SPNPSA1}=\underset{\sim}{S}_{32}=\{1/0,01;\ 0,2/0,1;\ 0/1\},$$
$$\underset{\sim}{T}_{322}=\underset{\sim}{T}_{SPNPSA2}=\underset{\sim}{A}_{32}=$$
$$\{0,5/0,01;\ 1/0,1;\ 0,7/1\},$$
$$\underset{\sim}{T}_{323}=\underset{\sim}{T}_{SPNPSA3}=\underset{\sim}{B}_{32}=\{0/0,01;\ 0,5/0,1;\ 0/1\}.$$

Stage 5 – formation of reference FN. To implement this step we use the fuzzy subset (linguistic) reference standards $\mathbf{T^e_{ij}}$ (see (13) in [2]), each of which displays a characteristic judgment of the expert (see step 1) regarding the anomalous state of the parameter P_{ij}.

Formation of fuzzy standards is based on the conversion of the corresponding FN (25) of the

Journal of Theoretical and Applied Information Technology
20th May 2016. Vol.87. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

subset $\mathbf{T_{ij}} \subseteq \mathbf{T}$ and is implemented through three steps.

Step 1. The transformation of the fuzzy terms (25) so that for all $\underset{\sim}{T}_{ijs}$ it was fair for the order relation, i.e. $\forall x_{ijsq} : x_{ijsq} < x_{ijsq+1}$ $(q = \overline{1, r_j - 1})$.

Step 2. Each $\underset{\sim}{T}_{ijs}$ is absorption ingredient $0/x_{ijs}^{min}$ and $0/x_{ijs}^{max}$ accordingly, a number of other components according to the expressions $x_{ijs}^{min} = \bigvee_{\substack{q=1 \\ npu\ U1}}^{M-1} x_{ijsq}$ and $x_{ijs}^{max} = \bigwedge_{\substack{q=M \\ npu\ U2}}^{r_j} x_{ijsq}$, where $U_1 \overset{def}{=} \forall x_{ijsq} < x_{ijsM} : \mu_{ijsq} = 0$, $U_2 \overset{def}{=} \forall x_{ijsq} > x_{ijsM} : \mu_{ijsq} = 0$ and x_{ijsM} and M – respectively mode $\underset{\sim}{T}_{ijs}$ and its ordinal number.

Further, given these transformations and the expressions (25), we define a set of intermediate terms in the form

$$\underset{\sim}{T}'_{ijs} = \{ \mu_{ijs\beta} / x_{ijs\beta}, \ldots, \bigcup_{q=\beta+1}^{r_j-\gamma} \mu_{ijsq} / x_{ijsq}, \ldots, \mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1} \} = \{ \mu_{ijs\beta} / x_{ijs\beta}, \mu_{ijs\beta+1} / x_{ijs\beta+1}, \ldots, \mu_{ijsr_j-\gamma} / x_{ijsr_j-\gamma}, \mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1} \}, \quad (28)$$

where $\mu_{ijs\beta} / x_{ijs\beta} = 0 / x_{ijs\beta} = 0/x_{ijs}^{min}$ and $\mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1} = 0 / x_{ijsr_j-\gamma+1} = 0/x_{ijs}^{max}$, but β and γ – the number of absorbed $0 / x_{ijsq}$ accordingly, the left and right of $x_{ijs(M)}$.

Thus, are formed of a subset of the standards

$$\underset{\sim}{T}^e_{ijs} = \{ \bigcup_{q=1}^{r_{js}} \mu^e_{ijsq} / x^e_{ijsq} \} = \{ \mu^e_{ijs1} / x^e_{ijs1}, \mu^e_{ijs2} / x^e_{ijs2}, \ldots, \mu^e_{ijsr_{js}-1} / x^e_{ijsr_{js}-1}, \mu^e_{ijsr_{js}} / x^e_{ijsr_{js}} \}, \ (q = \overline{1, r_{js}}), \quad (29)$$

where $\mu^e_{ijs1} / x^e_{ijs1} = \mu_{ijs\beta} / x_{ijs\beta}$, $\mu^e_{ijs2} / x^e_{ijs2} = \mu_{ijs\beta+1} / x_{ijs\beta+1}, \ldots, \mu^e_{ijsr_{js}-1} / x^e_{ijsr_{js}-1} = \mu_{ijsr_j-\gamma} / x_{ijsr_j-\gamma}$, $\mu^e_{ijsr_{js}} / x^e_{ijsr_{js}} = \mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1}$, r_{js} $(s = \overline{1, r_j})$ – the number of components in $\underset{\sim}{T}^e_{ijs}$.

Step 3. If the implementation of the second step for the expression (28) $\exists\, \underset{\sim}{T}'_{ijs} : \{0/x_{ijs}^{min}\} \in \varnothing$ or $\exists\, \underset{\sim}{T}'_{ijs} : \{0/x_{ijs}^{max}\} \in \varnothing$ (i.e. $\mu_{ijs\beta} \neq 0$, $\mu_{ijsr_j-\gamma+1} \neq 0$), for such further terms the formation of a subset $\underset{\sim}{T}^e_{ijs}$ by extension $\underset{\sim}{T}'_{ijs}$ through the introduction of additional $\mu_{ijs\beta-1} / x_{ijs\beta-1}$ and $\mu_{ijsr_j-\gamma+2} / x_{ijsr_j-\gamma+2}$ then again the FN components are indexed from $q = 1$.

With this in mind, the sets of intermediate terms will be as follows

$$\underset{\sim}{T}'_{ijs} = \{ \mu_{ijs\beta-1} / x_{ijs\beta-1}, \mu_{ijs\beta} / x_{ijs\beta}, \ldots, \bigcup_{q=\beta+1}^{r_j-\gamma} \mu_{ijsq} / x_{ijsq}, \ldots, \mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1}, \mu_{ijsr_j-\gamma+2} / x_{ijsr_j-\gamma+2} \} = \{ \mu_{ijs\beta-1} / x_{ijs\beta-1}, \mu_{ijs\beta} / x_{ijs\beta}, \ldots, \mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1}, \mu_{ijsr_j-\gamma+2} / x_{ijsr_j-\gamma+2} \},$$

where $x_{ijs\beta-1} = x_{ijs\beta}$, $x_{ijsr_j-\gamma+2} = x_{ijsr_j-\gamma+1}$ and $\mu_{ijs\beta-1} = \mu_{ijsr_j-\gamma+2} = 0$.

Thus, the components of the subset of standards $\underset{\sim}{T}^e_{ijs}$ in the expression (29) will be determined as $\mu^e_{ijs1} / x^e_{ijs1} = \mu_{ijs\beta-1} / x_{ijs\beta-1}$, $\mu^e_{ijs2} / x^e_{ijs2} = \mu_{ijs\beta} / x_{ijs\beta}$, …, $\mu^e_{ijsr_{js}-1} / x^e_{ijsr_{js}-1} = \mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1}$, $\mu^e_{ijsr_{js}} / x^e_{ijsr_{js}} = \mu_{ijsr_j-\gamma+2} / x_{ijsr_j-\gamma+2}$.

Consider the process of formation of the reference FN on a concrete example, i.e. according to the expression (13) in [2] with $i = 3$, $j = 2$, $r_j = 3$ для $\{\underset{\sim}{T}_{321}, \underset{\sim}{T}_{322}, \underset{\sim}{T}_{323}\}$ we will form $\mathbf{T^e_{32}} \subseteq \mathbf{T^e}$ i.e.

$$\mathbf{T^e_{32}} = \{ \bigcup_{s=1}^{3} \underset{\sim}{T}^e_{32s} \} = \{ \underset{\sim}{T}^e_{321}, \underset{\sim}{T}^e_{322}, \underset{\sim}{T}^e_{323} \} = \{ \underset{\sim}{T}^e_{SPNPSA1}, \underset{\sim}{T}^e_{SPNPSA2}, \underset{\sim}{T}^e_{SPNPSA3} \} = \{ \underset{\sim}{S}^e_{32}, \underset{\sim}{A}^e_{32}, \underset{\sim}{B}^e_{32} \}, \ (s = \overline{1,3}),$$

where members of the subset $\mathbf{T^e_{32}}$ – $\underset{\sim}{S}^e_{32}$, $\underset{\sim}{A}^e_{32}$, $\underset{\sim}{B}^e_{32}$ are reference FN.

Step 1. Convert fuzzy terms $\underset{\sim}{S}_{32}$, $\underset{\sim}{A}_{32}$ and $\underset{\sim}{B}_{32}$ so that was true for all $\underset{\sim}{T}_{32s}$ the order relation, i.e. $\forall x_{32sq} : x_{32sq} < x_{32sq+1}$ $(q = \overline{1,2})$. If the components of these terms to use specific values

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

obtained in the example of stage 4, such an attitude will be true. For example, for $\underset{\sim}{S}_{32}$ this $x_{3211} < x_{3212} < x_{3213} = 0,01<0,1<1$.

Step 2. For $\underset{\sim}{S}_{32}$, $\underset{\sim}{A}_{32}$, $\underset{\sim}{B}_{32}$ condition U_1 and U_2 not performed and therefore the operation of the absorption is not carried out. With this in mind and the expression (28) define a set of intermediate terms in the form:

$$\underset{\sim}{T}'_{321} = \underset{\sim}{T}'_{SPNPSA1} = \underset{\sim}{S}'_{32} = \{\mu_{3211}/x_{3211}, \mu_{3212}/x_{3212}, \mu_{3213}/x_{3213}\} = \{1/0,01;\ 0,2/0,1;\ 0/1\},$$

$$\underset{\sim}{T}'_{322} = \underset{\sim}{T}'_{SPNPSA2} = \underset{\sim}{A}'_{32} = \{\mu_{3221}/x_{3221}, \mu_{3222}/x_{3222}, \mu_{3223}/x_{3223}\} = \{0,5/0,01;\ 1/0,1;\ 0,7/1\},$$

$$\underset{\sim}{T}'_{323} = \underset{\sim}{T}'_{SPNPSA3} = \underset{\sim}{B}'_{32} = \{\mu_{3231}/x_{3231}, \mu_{3232}/x_{3232}, \mu_{3233}/x_{3233}\} = \{0/0,01;\ 0,5/0,1;\ 1/1\}.$$

Step 3. For the second step in the expression (28) for a set of intermediate terms $\underset{\sim}{S}'_{32}$ and $\underset{\sim}{A}'_{32}$ $\exists\, \underset{\sim}{T}'_{321}:\{0/x^{min}_{321}\}\in\varnothing$ and $\exists\, \underset{\sim}{T}'_{322}:\{0/x^{min}_{322}\}\in\varnothing$ (т.е. $\mu_{3211}=1\neq 0$ and $\mu_{3221}=0,5\neq 0$), and for $\underset{\sim}{A}'_{32}$ and $\underset{\sim}{B}'_{32}$ $\exists\, \underset{\sim}{T}'_{322}:\{0/x^{max}_{322}\}\in\varnothing$ and $\exists\, \underset{\sim}{T}'_{323}$: $\{0/x^{max}_{323}\}\in\varnothing$ and (т.е. $\mu_{3223}=0,7\neq 0$ and $\mu_{3233}=1\neq 0$), the formation of subsets $\underset{\sim}{T}^e_{321}$, $\underset{\sim}{T}^e_{322}$ and $\underset{\sim}{T}^e_{323}$ feasible due to expansion $\underset{\sim}{T}'_{321}$, $\underset{\sim}{T}'_{322}$ and $\underset{\sim}{T}'_{323}$ (см. (28)) through the introduction of additional $\mu_{321\beta-1}/x_{321\beta-1} = 0/0,01$, $\mu_{322\beta-1}/x_{322\beta-1} = 0/0,01$, $\mu_{322r_j-\gamma+2}/x_{322r_j-\gamma+2} = 0/1$ and $\mu_{323r_j-\gamma+2}/x_{323r_j-\gamma+2} = 0/1$ respectively, then FN is the reindex component from the first.

With this in mind, a set of intermediate terms for $\underset{\sim}{S}'_{32}$ will be as follows

$$\underset{\sim}{T}'_{321} = \underset{\sim}{T}'_{SPNPSA1} = \underset{\sim}{S}'_{32} = \{\mu_{3211}/x_{3211}, \mu_{3212}/x_{3212}, \mu_{3213}/x_{3213}, \mu_{3214}/x_{3214}\} = \{0/0,01;\ 1/0,01;\ 0,2/0,1;\ 0/1\},$$

where $\mu_{321\beta-1}=0$. Same way the intermediate baths for $\underset{\sim}{A}'_{32}$ and $\underset{\sim}{B}'_{32}$ where $\mu_{322\beta-1} = \mu_{322r_j-\gamma+2} = \mu_{323r_j-\gamma+2} = 0$.

Thus, the components of the subset of standards $\underset{\sim}{T}^e_{321}$ according to expression (29) will be determined as $\mu^e_{3211}/x^e_{3211} = 0/0,01$, $\mu^e_{3212}/x^e_{3212} = 1/0,01$, $\mu^e_{3213}/x^e_{3213} = 0,2/0,1$, $\mu^e_{3214}/x^e_{3214} = 0/1$ and similarly for $\underset{\sim}{T}^e_{322}$ and $\underset{\sim}{T}^e_{323}$.

Further, according to expressions (29) for $\underset{\sim}{S}'_{32}$, $\underset{\sim}{A}'_{32}$ and $\underset{\sim}{B}'_{32}$ may form a reference value, i.e.:

$$\underset{\sim}{T}^e_{321} = \underset{\sim}{T}^e_{SPNPSA1} = \underset{\sim}{S}^e_{32} = \{\mu^e_{3211}/x^e_{3211}, \mu^e_{3212}/x^e_{3212}, \mu^e_{3213}/x^e_{3213}, \mu^e_{3214}/x^e_{3214}\} = \{0/0,01;\ 1/0,01;\ 0,2/0,1;\ 0/1\},$$

$$\underset{\sim}{T}^e_{322} = \underset{\sim}{T}^e_{SPNPSA2} = \underset{\sim}{A}^e_{32} = \{\mu^e_{3221}/x^e_{3221}, \mu^e_{3222}/x^e_{3222}, \mu^e_{3223}/x^e_{3223}, \mu^e_{3224}/x^e_{3224}, \mu^e_{3225}/x^e_{3225}\} = \{0/0,01;\ 0,5/0,01;\ 1/0,1;\ 0,7/1;\ 0/1\},$$

$$\underset{\sim}{T}^e_{323} = \underset{\sim}{T}^e_{SPNPSA3} = \underset{\sim}{B}'_{32} = \{\mu^e_{3231}/x^e_{3231}, \mu^e_{3232}/x^e_{3232}, \mu^e_{3233}/x^e_{3233}, \mu^e_{3234}/x^e_{3234}\} = \{0/0,01;\ 0,5/0,1;\ 1/1;\ 0/1\},$$

where for example: $\mu^e_{3231}/x^e_{3231} = \mu_{3231}/x_{3231}$, $\mu^e_{3232}/x^e_{3232} = \mu_{3232}/x_{3232}$, $\mu^e_{3233}/x^e_{3233} = \mu_{3233}/x_{3233}$ and $\mu^e_{3234}/x^e_{3234} = \mu_{3234}/x_{3234}$. From the example it is obvious that $r_1 = r_3 = 4$, $r_2 = 5$.

Stage 6 – visualization of linguistic standards. Implementation of this phase is based on building a geometric image of all reference FN (29) belonging to the subset $\mathbf{T}^{\mathbf{e}}_{\mathbf{ij}}$ (see (13) in [2]). The locus of points in the plane is defined by a polyline connecting the points representing the components of FN $\underset{\sim}{T}^e_{ijs}$ in ascending order of their supports (media) x^e_{ijsq}. Visualization of one standard reference term (29) is presented in the broken line form —●— on figure 1.

For example, to visualize only a subset of the standards $\mathbf{T}^{\mathbf{e}}_{\mathbf{32}} = \mathbf{T}^{\mathbf{e}}_{\mathbf{SPNPSA}}$ FN will use the reference generated in step 5 (see example):

Journal of Theoretical and Applied Information Technology
20th May 2016. Vol.87. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$\underset{\sim}{S}^{e}_{32} = \{0/0{,}01;\ 1/0{,}01;\ 0{,}2/0{,}1;\ 0/1\}$,

$\underset{\sim}{A}^{e}_{32} = \{0/0{,}01;\ 0{,}5/0{,}01;\ 1/0{,}1;\ 0{,}7/1;\ 0/1\}$,

$\underset{\sim}{B}^{e}_{32} = \{0/0{,}01;\ 0{,}5/0{,}1;\ 1/1;\ 0/1\}$.

Based on them by joining the points that appear relevant parts of the reference FN $\underset{\sim}{S}^{e}_{32}$, $\underset{\sim}{A}^{e}_{32}$, $\underset{\sim}{B}^{e}_{32}$ five broken lines are under construction —●—, —■—, —○—, —□—, —◫—, which is graphically interpreted in figure 2.

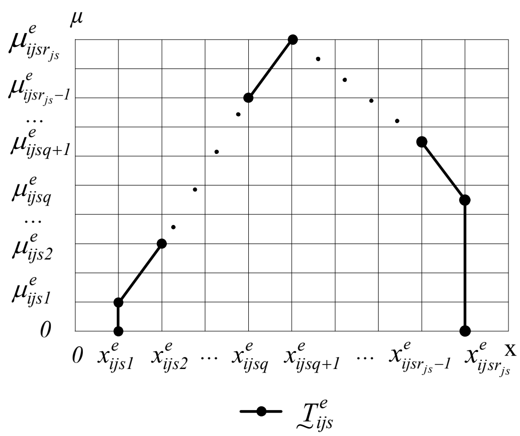

Figure 1. The Linguistic Standard Bass $\underset{\sim}{T}^{e}_{ijs}$

Figure 2. The Linguistic Standards Of The Subset

$\mathbf{T}^{e}_{SPNPSA}$

3. CONCLUSIONS

The proposed improved MFLS for intrusion detection systems, which through the use of sets of identifiers of linguistic assessments and of the identifiers of intervals, basic and derivative matrix frequency display of the judgments of experts regarding cyberattacks characterizing the current state of the settings and processes of formation at given intervals of frequencies of occurrence of expert assessments and subsets in fuzzy terms, allows to formalize the procedure of obtaining reference values of the parameters specified groups of linguistic variables, characterizing in various conditions of the anomalous specific parametric heterogeneous environment.

The proposed MFLS is part of the basic tuple model [2], [24], as well as the theoretical Foundation for building systems intrusion detection on fuzzy logic. The proposed MPLA is part of the basic tuple model [2], [24], as well as the theoretical Foundation for building systems intrusion detection on fuzzy logic.

REFRENCES:

[1]. Korchenko A.A. The model of heuristic rules on the set of logical-linguistic tangles for abnormality detection in computer systems, Zahist іnformacії, 2012, №4 (57), pp. 112-118. (in Russian)

[2]. Korchenko A.A. The tupel model of basic components' set formation for cyberattacks, Legal, regulatory and metrological support information security system in Ukraine, 2014, V.2 (28), pp. 29-36. (in Russian)

[3]. Yao J.T., Zhao S.L., Saxton L.V. «A study on fuzzy intrusion detection» Proc. of SPIE Data Mining, Intrusion Detection, Information Assurance, And Data Networks Security, Orlando, Florida, USA, Vol. 5812, 2005, pp. 23-30.

[4]. Fries P. «A Fuzzy-Genetic Approach to Network Intrusion Detection Terrence» Genetic and Evolutionary Computation Conference, GECCO (Companion) July 12-16, 2008, pp. 2141-2146.

[5]. A Fuzzy Approach For Detecting Anomalous Behaviour in E-mail Traffic [Electronic resource] / Mark JynHuey Lim, Michael Negnevitsky, Jacky Hartnett // About Research Online @ ECU. – Electronic data. – Perth Western Australia] : Edith Cowan University, 2006. – Mode of access: World Wide Web. – URL: http://ro.ecu.edu.au/adf/29/. – Title from title screen. – Description based on home page (viewed on May 26, 2015).

[6]. Stasiuk A.I., Korchenko A.A. The basic model of parameters in attack detection (Identification) systems construction, Zahist іnformacії, 2012, №2 (55), pp. 47-51. (in Russian)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[7]. Lutskiy M.G., Korchenko A.A., Gavrylenko A.V., Okhrimenko A.A. The models of linguistic variables for attack detection systems, Zahist ìnformacìï, 2012, №2 (55), pp. 71-78. (in Russian)
[8]. Wijayasekara D., Linda O., Manic M., Rieger C.G. Mining Building Energy Management System Data Using Fuzzy Anomaly Detection and Linguistic Descriptions. IEEE Trans. Industrial Informatics. Vol. 10, № 3, 2014, pp 1829-1840.
[9]. Stasiuk A.I., Korchenko A.A. A method of abnormality detection caused by cyber attacks in computer networks, Zahist ìnformacìï, 2012, №4 (57), pp. 129-134. (in Russian)
[10]. Korchenko A.A. The formation method of linguistic standards created for the intrusion detection systems, Zahist ìnformacìï, T.16, №1, 2014, pp. 5-12. (in Russian)
[11]. Korchenko A.A. Anomaly-based detection system in computer networks, Bezpeka ìnformacìï, 2012, №2 (18), pp. 80-84. (in Russian)
[12]. Korchenko A.A. The system development of fuzzy standards of network parameters, Zahist ìnformacìï, T.15, №3, 2013, pp. 240-246. (in Russian)
[13]. Korchenko A.A. The system of heuristic rules formation for network activity assessment, Zahist ìnformacìï, T.15, №4, 2013, pp. 353-359. (in Russian)
[14]. Shanmugavadivu R., Nagarajan N. «Network Intrusion Detection System Using Fuzzy Logic», Indian Journal of Computer Science and Engineering (IJCSE), Vol. 2, No. 1, pp. 101-111, 2011.
[15]. Linda O., Vollmer T., Wright J., Manic M. «Fuzzy Logic Based Anomaly Detection for Embedded Network Security Cyber Sensor», in Proc. IEEE Symposium Series on Computational Intelligence, Paris, France, April, 2011, pp. 202-209.
[16]. Bridges S.M., Vaughn R.B. «Fuzzy data mining and genetic algorithms applied to intrusion detection». In: Proceedings of the 23rd National Information Systems Security Conference. October 2000, pp. 13-31.
[17]. Shahaboddin Shamshirband, Nor Badrul Anuar, Miss Laiha, Mat Kiah, Sanjay Misra «Anomaly Detection using Fuzzy Q-learning Algorithm» Acta Polytechnica Hungarica. Vol. 11, № 8, 2014, pp. 5-28.
[18]. John E. Dickerson, Jukka Juslin, Ourania Koukousoula, Julie A. Dickerson «Fuzzy Intrusion Detection» IFSA World Congress and 20th NAFIPS International Conference, 2001. Joint 9th. Vol. 3, pp. 1506-1510.
[19]. Chi-Ho Tsang, Sam Kwong, Hanli Wang « Genetic-Fuzzy Rule Mining Approach and Evaluation of Feature Selection Techniques for Anomaly Intrusion Detection » Pattern Recognition, Vol. 40, №. 9, Sept. 2007, pp. 2373-2391.
[20]. Zadeh L.A. «Outline of a New Approach to the Analysis of Complex Systems and Decision Processes» IEEE Transactions on Systems, Man, and Cybernetics, Vol. SMC-3, №. 1, January 1973, pp. 28-44.
[21]. Gómez J., González F., Dasgupta D. «An Immuno-Fuzzy Approach to Anomaly Detection» The 12th IEEE International Conference on Fuzzy Systems, FUZZ-IEEE 25-28 May 2003, pp. 1219-1224.
[22]. Mohammed Ali Tawfiq «Security Measurements of Internet Website Zone for IE9 Based on Fuzzy Logic» Journal of Engineering and Development. Vol. 17, № 1, Mar. 2013, pp. 255-269.
[23]. Korchenko A.G. The development of information protection systems based on the fuzzy sets, The theory and practical solutions, Kuev, 2006, 320 p. (in Russian)
[24]. Anna Korchenko, Kornel Warwas, Aleksandra Kłos-Witkowska. The Tupel Model of Basic Components' Set Formation for Cyberattacks // Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015), Warsaw, Poland, September 24-26, 2015: Vol. 1. – pp. 478-483.