Journal of Theoretical and Applied Information Technology
31st August 2019. Vol.97. No 16

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

DETECTION ENVIRONMENT FORMATION METHOD FOR ANOMALY DETECTION SYSTEMS

[1] NAZYM ZHUMANGALIYEVA, [2] ANNA KORCHENKO, [3] ALIYA DOSZHANOVA, [4] AIGUL SHAIKHANOVA, [5] SHANGYTBAYEVA GULMIRA [6] AVKUROVA ZHADYRA.

[1] Kazakh National Research Technical University after K.I. Satpayev, [2,] Department of Information Technology Security, National Aviation University, Kyiv, Ukraine [3,]Almaty University of Power Engineering and Telecommunications , [4,] Shakarim State University of the City of Semey ,[5] K.Zhubanov Aktobe Regional State University, [6] L.N.Gumilyov Eurasian National University

E-mail: [1]nazym_k.81@mail.ru,[2]annakor@ukr.net, [3]d_alia.81@mail.ru. [4]igul7@mail.ru [5]gul_janet@mail.ru, [6]zhadyra.avkurova.83@mail.ru

ABSTRACT

Due to the intensive development of the digital business, malicious software and other cyber threats are becoming more common. In order to increase the level of security there are needed appropriate special countermeasures, which are able to remain effective when new types of threats occur and which allow to detect cyber attacks targeting on a set of information system resources in fuzzy conditions. Different attacking effects on the corresponding resources generate various sets of anomalies in a heterogeneous parametric environment. There is known a tuple model of the formation of a set of basic components that allow to identify cyber attacks. For its effective application a formal implementation of the approach to the formation of sets of basic detection rules is necessary. For this purpose, there has been developed a method that focuses on solving problems of cyber attacks detection in computer systems, which is implemented through three basic steps: formation of anomaly identifiers subsets; formation of decisive functions; formation of conditional detection expressions. Using this method, it is possible to form the necessary set of detection rules, which determine the level of anomalous state of values in a heterogeneous parametric environment, characteristic for the impact of a certain type of attack. The use of this method at the creation intrusion detection systems will expand their functionality regarding the cyber attacks detection in a weakly formalized fuzzy environment.

Keywords: *detection rules, attacks, cyber attacks, anomalies, intrusion detection systems, anomaly detection systems, attack detection systems.*

1. RELEVANCE

Nowadays, the intensive development, as well as the enormous scale and rate of information technology implementation in modern business have become a natural process for developed corporations. The level of company informatization is one of the main factors for its successful development, and in the conditions of a large market dynamism and complication of its infrastructure, information becomes a strategic resource. The development of information technologies is being transformed so quickly that the classic protection mechanisms cannot remain effective and provide adequate security for information system resources, and malicious software and other cyber threats are becoming more common. In this regard, there are needed special tools in order to detect and to prevent security breaches. Intrusion detection systems are used for this, which are an integral part of any serious security system, and the global trend is that intrusion and anomalies detection will become a mandatory function of any operating system and will already be used in various software. Expanding the functionality of such systems by identifying previously unknown cyber attacks characterized by unspecified or unclearly defined criteria will allow actually to remain functional in a weakly formalized fuzzy environment. The use of the necessary methods, models and methodologies of information security based on fuzzy sets for the creation of appropriate means of detecting intrusions and anomalies is the basis for successfully countering to these cyber attacks. One of the important stages in the anomalies detection is the creation of fuzzy (detection) rules [1]-[10].

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

According to this, the actual scientific task is the formalization of the detection rules creation process, which make it possible to detect cyber attacks targeting on various information system resources in fuzzy conditions.

2.. ANALYSIS OF EXISTING RESEARCH

Effective security tools used to solve problems of cyber attacks detection are: the tuple model for generating a set of basic components for cyber attacks detection [11], fuzzy approaches for intrusions detection [12]-[13] and for anomalies detection [14]; corresponding fuzzy models [11], [15], methods [16]-[23] and intrusion detection systems [24]-[27]; sets of fuzzy rules [1]-[10]; as well as other developments used to solve protection problems under fuzzy conditions [28], [29]. These researches have shown the effectiveness of using the mathematical apparatus of fuzzy sets, and its use in order to formalize the approach for cyber attacks identifying will improve the process of creating appropriate intrusion detection systems. It should be noted that the set of attacking effects on the information systems resources gives a rise to many anomalies among the values in a heterogeneous parametric environment [11], [15]. For an effective application of the well-known model [11], a formal implementation of the formation process of sets of basic detection rules is necessary, which will allow searching for an identifying term [17], [21]-[23] in a given linguistic variable. Using this term, using the appropriate set of rules, we can determine the level of the anomalous state generated by the influence of the corresponding class of cyber attacks.

3. MAIN OBJECTIVE OF RESEARCH

On the basis of the analysis of existing researches and the relevance of the task, the main objective of this work is to develop a detection environment formation method (DEFM) for anomaly detection systems operating in a weakly formalized fuzzy environment. Using this method (at solving problems of cyber attacks detection), it is possible effectively to detect the level of the anomalous state characteristic for a certain type of attacks regarding to a specific heterogeneous parametric environment in a given time interval.

4. MAIN PART OF RESEARCH

In order to create subsets of the basic detection rules $\mathbf{DR}_i$ (see (19) in [11]), we will develop an appropriate method that will allow to formalize the process of obtaining the corresponding rules used to detect the i-th cyber attack based on parametric sub-environments of various dimensions [11], [15]. The proposed DEFM is focused on solving problems of attacks detection in computer systems, and is based on three stages: formation of anomaly identifiers subsets; formation of decisive functions; formation of conditional detection expressions.

Stage 1 – formation of anomaly identifiers subsets.

The subset $\mathbf{IA}_i$ is built on the basis of the set of all possible $\mathbf{IA}$ anomaly identifiers (ID), represented as

$$\mathbf{IA} = \{\bigcup_{o=1}^{\xi} IA_o\} = \{IA_1, IA_2, \ldots, AI_\xi\}, \quad (o = \overline{1,\xi}), \tag{1}$$

and by means of which (in linguistic form) it is possible to display possible levels of an anomalous state in a m-dimensional heterogeneous parametric environment that can be generated by a cyber attack with ID CA_i [11], and ξ – an amount of anomaly ID.

For example, at $\xi = 9$ according to (1) the set $\mathbf{IA}$ can be represented as follows:

$$\mathbf{IA} = \{\bigcup_{o=1}^{9} IA_o\} = \{IA_1, IA_2, \ldots, AI_9\} = \{IA_H, IA_{БНВ}, IA_{НС}, IA_C, IA_{ВС}, IA_{БВН}, IA_B, IA_П, IA_Г\} = \{"Н", "БНВ", "НС", "С", "ВС", "БВН", "В", "П", "Г"\} \tag{2}$$

where: $IA_1 = IA_H = "Н"$, $IA_2 = IA_{БНВ} = "БНВ"$, $IA_3 = IA_{НС} = "НС"$, $IA_4 = IA_C = "С"$, $IA_5 = IA_{ВС} = "ВС"$, $IA_6 = IA_{БВН} = "БВН"$, $IA_7 = IA_B = "В"$, $IA_8 = IA_П = "П"$, $IA_9 = IA_Г = "Г"$ are respectively the anomaly IDs by which in linguistic forms: “LOW (L)” (at $\xi = 1$), “MORE LOW THAN HIGH (MLTH)” (at $\xi = 2$), “BELOW AVERAGE (BA)” (at $\xi = 3$), “AVERAGE (A)” (at $\xi = 4$), “ABOVE AVERAGE (AA)” (at $\xi = 5$), “MORE HIGH THAN LOW (MHTL) (at $\xi = 6$), “HIGH (H)” (at $\xi = 7$), “LIMIT (L)” (at $\xi = 8$), “BOUNDARY (B)” (at $\xi = 9$), possible anomaly levels can be displayed.

Next, we form a subset of the anomaly ID for the subset of rules $\mathbf{DR}_i$ [11] i.e.:

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

$$\{\bigcup_{i=1}^{n}\mathbf{IA_i}\}=\{\mathbf{IA_1},\ \mathbf{IA_2},\ \ldots,\ \mathbf{IA_n}\},\quad (i=\overline{1,n}), \tag{3}$$

where $\mathbf{IA_i} \subseteq \mathbf{IA}$ will be defined as:

$$\mathbf{IA_i}=\{\bigcup_{u=1}^{v_i} IA_{iu}\}=\{IA_{i1},\ IA_{i2},\ \ldots,\ IA_{iv_i}\},\quad (u=\overline{1,v_i}), \tag{4}$$

in this case v_i denotes the amount of anomaly IDs, by which in linguistic forms it is possible to display possible anomaly levels generated by cyber attacks with ID CA_i. Therefore, an expression (3) taking into account (4) will be represented in the following form:

$$\{\bigcup_{i=1}^{n}\mathbf{IA_i}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{u=1}^{v_i} IA_{iu}\}\}=$$
$$\{\{IA_{11},\ IA_{12},\ \ldots,\ IA_{1v_1}\},\{IA_{21},\ IA_{22},\ \ldots,\ IA_{2v_2}\},$$
$$\ldots,$$
$$\{IA_{n1},\ IA_{n2},\ \ldots,\ AI_{nv_n}\}\}. \tag{5}$$

For example, at $n=3$ (i.e. for cyber attacks with ID $CA_1=CA_{SN}=SN$, $CA_2=CA_{DS}=DS$ and $CA_3=CA_{SP}=SP$) and $v_1=v_2=v_3=5$ taking into account (1), we define the necessary IDs in order to display the corresponding anomaly level. Then the expression (5) taking into account (2) will have the following form:

$$\{\bigcup_{i=1}^{3}\mathbf{IA_i}\}=\{\bigcup_{i=1}^{3}\{\bigcup_{u=1}^{v_i} IA_{iu}\}\}=$$
$$\{\{IA_{11},\ IA_{12},\ IA_{13},\ IA_{14},\ IA_{15}\},$$
$$\{IA_{21},\ IA_{22},\ IA_{23},\ IA_{24},\ IA_{25}\},$$
$$\{IA_{31},\ IA_{32},\ IA_{33},\ IA_{34},\ IA_{35}\}\}=$$
$$\{\{IA_{SNH},\ IA_{SNБHB},\ IA_{SNБBH},\ IA_{SNB},\ IA_{SNП}\},$$
$$\{IA_{DSH},\ IA_{DSБHB},\ IA_{DSБBH},\ IA_{DSB},\ IA_{DSП}\},$$
$$\{IA_{SPH},\ IA_{SPБHB},\ IA_{SPБBH},\ IA_{SPB},\ IA_{SPП}\}\}=$$
$$\{\{"Н",\ "БНВ",\ "ББН",\ "В",\ "П"\},$$
$$\{"Н",\ "БНВ",\ "ББН",\ "В",\ "П"\},$$
$$\{"Н",\ "БНВ",\ "ББН",\ "В",\ "П"\}\}, \tag{6}$$

where: SN – Scanning of ports, DS – Denial of service, SP – Spoofing, as well as $IA_{11}=IA_{SNH}="Н"$, $IA_{12}=IA_{SNБHB}="БНВ"$, $IA_{13}=IA_{SNБBH}="ББН"$, $IA_{14}=IA_{SNB}="В"$, $IA_{15}=IA_{SNП}="П"$, respectively, the IDs of such anomalous states in the attacking environment, which represent a different degree of expert confidence regarding to the influence of a cyber attack with an ID $CA_1=CA_{SN}$ [11]; $IA_{21}=IA_{DSH}="Н"$, $IA_{22}=IA_{DSБHB}="БНВ"$, $IA_{23}=IA_{DSБBH}="ББН"$, $IA_{24}=IA_{DSB}="В"$, $IA_{25}=IA_{DSП}="П"$ $IA_{15}=IA_{SNП}="П"$, respectively, the IDs of such anomalous states in the attacking environment, which represent a different degree of expert confidence regarding to the influence of a cyber attack with an ID $CA_2=CA_{DS}$; $IA_{31}=IA_{SPH}="Н"$, $IA_{32}=IA_{SPБHB}="БНВ"$, $IA_{33}=IA_{SPБBH}="ББН"$, $IA_{34}=IA_{SPB}="В"$, $IA_{35}=IA_{SPП}="П"$ $IA_{15}=IA_{SNП}="П"$, respectively, the IDs of such anomalous states in the attacking environment, which represent a different degree of expert confidence regarding to the influence of a cyber attack with an ID $CA_3=CA_{SP}$.

Stage 2 – formation of decisive functions.

In order to implement this stage, we introduce the set of all arguments of the decisive functions $\mathbf{AF}$ and a subset of such arguments $\mathbf{AF_i}$.

$$\{\bigcup_{i=1}^{n}\mathbf{AF_i}\}=\{\mathbf{AF_1},\ \mathbf{AF_2},\ \ldots,\ \mathbf{AF_n}\},\quad (i=\overline{1,n}), \tag{7}$$

where $\mathbf{AF_i} \subseteq \mathbf{AF}$, will be defined as:

$$\mathbf{AF_i}=\{\bigtimes_{a=1}^{w_i}\mathbf{AF_{ia}}\}=\{\mathbf{AF_{i1}}\times\mathbf{AF_{i2}}\times\ldots\times\mathbf{AF_{iw_i}}\},\quad (a=\overline{1,w_i}), \tag{8}$$

in this case w_i – the amount of subsets of arguments of the decisive functions used to detect the i-th cyber attack, and the symbol $\times$ indicates the direct composition of the sets. Taking into account the expression (8) the formula (7) will be written in the following form:

$$\{\bigcup_{i=1}^{n}\mathbf{AF_i}\}=\{\bigcup_{i=1}^{n}\{\bigtimes_{a=1}^{w_i}\mathbf{AF_{ia}}\}\}=$$
$$\{\{\mathbf{AF_{11}},\ \mathbf{AF_{12}},\ \ldots,\ \mathbf{AF_{1w_1}}\}\times$$
$$\{\mathbf{AF_{21}},\ \mathbf{AF_{22}},\ \ldots,\ \mathbf{AF_{2w_2}}\}\times\ldots\times$$
$$\{\mathbf{AF_{n1}},\ \mathbf{AF_{n2}},\ \ldots,\ \mathbf{AF_{nw_n}}\},$$
$$(i=\overline{1,n},\ a=\overline{1,w_i}), \tag{9}$$

The subset $\mathbf{AF_{ia}} \subseteq \mathbf{AF_i}$ will be defined as:

$$\mathbf{AF_{ia}}=\{\bigcup_{s=1}^{r_j} AF_{ias}\}=$$

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

$$\{ AF_{ia1}, AF_{ia2}, ..., AF_{iar_j} \}, (s = \overline{1, r_j}) \quad (10)$$

where r_j – amount of units in $\mathbf{AF_{ia}}$ (that displays the amount of units in $\mathbf{T^e_{ij}}$ (see (13) in [11])).

Then the expression (9) taking into account (10) takes the following form:

$$\{\bigcup_{i=1}^{n} \mathbf{AF_i}\} = \{\bigcup_{i=1}^{n} \{\times_{a=1}^{w_i} \mathbf{AF_{ia}}\}\} = \{\bigcup_{i=1}^{n} \{\times_{a=1}^{w_i} \{\bigcup_{s=1}^{r_j} AF_{ias}\}\}\} =$$

$$\{\{\{ AF_{111}, AF_{112}, ..., AF_{11r_j} \} \times \{ AF_{121}, AF_{122}, ..., AF_{12r_j} \} \times ... \times \{ AF_{1w_1 1}, AF_{1w_1 2}, ..., AF_{1w_1 r_j} \}\},$$

$$\{\{ AF_{211}, AF_{212}, ..., AF_{21r_j} \} \times \{ AF_{221}, AF_{222}, ..., AF_{22r_j} \} \times ... \times \{ AF_{2w_2 1}, AF_{2w_2 2}, ..., AF_{2w_2 r_j} \}\}, ...,$$

$$\{\{ AF_{n11}, AF_{n12}, ..., AF_{n1r_j} \} \times \{ AF_{n21}, AF_{n22}, ..., AF_{n2r_j} \} \times ... \times \{ AF_{nw_n 1}, AF_{nw_n 2}, ..., AF_{nw_n r_j} \}\} =$$

$$\{\{\langle AF_{111}, AF_{121}, ..., AF_{1w_1 1} \rangle, \langle AF_{111}, AF_{121}, ..., AF_{1w_1 2} \rangle, ..., \langle AF_{111}, AF_{121}, ..., AF_{1w_1 r_1} \rangle,$$

$$\langle AF_{111}, AF_{122}, ..., AF_{1w_1 1} \rangle, \langle AF_{111}, AF_{122}, ..., AF_{1w_1 2} \rangle, ..., \langle AF_{111}, AF_{122}, ..., AF_{1w_1 r_1} \rangle, ...,$$

$$\langle AF_{111}, AF_{12r_2}, ..., AF_{1w_1 1} \rangle, \langle AF_{111}, AF_{12r_2}, ..., AF_{1w_1 2} \rangle, ..., \langle AF_{111}, AF_{12r_2}, ..., AF_{1w_1 r_1} \rangle,$$

$$\langle AF_{112}, AF_{121}, ..., AF_{1w_1 1} \rangle, \langle AF_{112}, AF_{121}, ..., AF_{1w_1 2} \rangle, ..., \langle AF_{112}, AF_{121}, ..., AF_{1w_1 r_1} \rangle,$$

$$\langle AF_{112}, AF_{122}, ..., AF_{1w_1 1} \rangle, \langle AF_{112}, AF_{122}, ..., AF_{1w_1 2} \rangle, ..., \langle AF_{112}, AF_{122}, ..., AF_{1w_1 r_1} \rangle, ...,$$

$$\langle AF_{112}, AF_{12r_2}, ..., AF_{1w_1 1} \rangle, \langle AF_{112}, AF_{12r_2}, ..., AF_{1w_1 2} \rangle, ..., \langle AF_{112}, AF_{12r_2}, ..., AF_{1w_1 r_1} \rangle, ...,$$

$$\langle AF_{11r_1}, AF_{121}, ..., AF_{1w_1 1} \rangle, \langle AF_{11r_1}, AF_{121}, ..., AF_{1w_1 2} \rangle, ..., \langle AF_{11r_1}, AF_{121}, ..., AF_{1w_1 r_1} \rangle,$$

$$\langle AF_{11r_1}, AF_{122}, ..., AF_{1w_1 1} \rangle, \langle AF_{11r_1}, AF_{122}, ..., AF_{1w_1 2} \rangle, ..., \langle AF_{11r_1}, AF_{122}, ..., AF_{1w_1 r_1} \rangle, ...,$$

$$\langle AF_{11r_1}, AF_{12r_2}, ..., AF_{1w_1 1} \rangle, \langle AF_{11r_1}, AF_{12r_2}, ..., AF_{1w_1 2} \rangle, ..., \langle AF_{11r_1}, AF_{12r_2}, ..., AF_{1w_1 r_1} \rangle\},$$

...,

$$\{\langle AF_{n11}, AF_{n21}, ..., AF_{nw_n 1} \rangle, \langle AF_{n11}, AF_{n21}, ..., AF_{nw_n 2} \rangle, ..., \langle AF_{n11}, AF_{n21}, ..., AF_{nw_n r_j} \rangle,$$

$$\langle AF_{n11}, AF_{n22}, ..., AF_{nw_n 1} \rangle, \langle AF_{n11}, AF_{n22}, ..., AF_{nw_n 2} \rangle, ..., \langle AF_{n11}, AF_{n22}, ..., AF_{nw_n r_j} \rangle, ...,$$

$$\langle AF_{n11}, AF_{n2r_2}, ..., AF_{nw_n 1} \rangle, \langle AF_{n11}, AF_{n2r_2}, ..., AF_{nw_n 2} \rangle, ..., \langle AF_{n11}, AF_{n2r_2}, ..., AF_{nw_n r_j} \rangle,$$

$$\langle AF_{n12}, AF_{n21}, ..., AF_{nw_n 1} \rangle, \langle AF_{n12}, AF_{n21}, ..., AF_{nw_n 2} \rangle, ..., \langle AF_{n12}, AF_{n21}, ..., AF_{nw_n r_j} \rangle,$$

$$\langle AF_{n12}, AF_{n22}, ..., AF_{nw_n 1} \rangle, \langle AF_{n12}, AF_{n22}, ..., AF_{nw_n 2} \rangle, ..., \langle AF_{n12}, AF_{n22}, ..., AF_{nw_n r_j} \rangle, ...,$$

$$\langle AF_{n12}, AF_{n2r_2}, ..., AF_{nw_n 1} \rangle, \langle AF_{n12}, AF_{n2r_2}, ..., AF_{nw_n 2} \rangle, ..., \langle AF_{n12}, AF_{n2r_2}, ..., AF_{nw_n r_j} \rangle,$$

...,

$$\langle AF_{n1r_1}, AF_{n21}, ..., AF_{nw_n 1} \rangle, \langle AF_{n1r_1}, AF_{n21}, ..., AF_{nw_n 2} \rangle, ..., \langle AF_{n1r_1}, AF_{n21}, ..., AF_{nw_n r_j} \rangle,$$

$$\langle AF_{n1r_1}, AF_{n22}, ..., AF_{nw_n 1} \rangle, \langle AF_{n1r_1}, AF_{n22}, ..., AF_{nw_n 2} \rangle, ..., \langle AF_{n1r_1}, AF_{n22}, ..., AF_{nw_n r_j} \rangle,$$

...,

$$\langle AF_{n1r_1}, AF_{n2r_2}, ..., AF_{nw_n 1} \rangle, \langle AF_{n1r_1}, AF_{n2r_2}, ..., AF_{nw_n 2} \rangle, ..., \langle AF_{n1r_1}, AF_{n2r_2}, ..., AF_{nw_n r_j} \rangle\}\} =$$

$$\{\{\langle \mathbf{SAF_{11}} \rangle, \langle \mathbf{SAF_{12}} \rangle, ..., \langle \mathbf{SAF_{1w_1}} \rangle\}, ..., \{\langle \mathbf{SAF_{i1}} \rangle, \langle \mathbf{SAF_{i2}} \rangle, ..., \langle \mathbf{SAF_{iw_i}} \rangle\}, ...,$$

$$\{\langle \mathbf{SAF_{n1}} \rangle, \langle \mathbf{SAF_{n2}} \rangle, ..., \langle \mathbf{SAF_{nw_n}} \rangle\}\}, \quad (11)$$

where, for clarity, there are used angle brackets "$\langle$", "$\rangle$", which separate the subsets of arguments of the decisive functions ($\mathbf{SAF_{ia}}$), which reflect the values of terms $\mathbf{T^{ep}_{ij}}$.

Taking into account the expression (11), we determine that in order to identify the i-th cyber attack, the total amount of argument subsets is calculated using the formula

$$w_i = \prod_{j=1}^{m_i} r_j, (j = \overline{1, m_i}). \quad (12)$$

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

Then (11) taking into account (12) it can be written in the following form

$$\{\bigcup_{i=1}^{n}\mathbf{AF_i}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{a=1}^{w_i}\langle\mathbf{SAF_{ia}}\rangle\}\},\ (a=\overline{1,w_i}) \quad (13)$$

Next, we introduce the set of all binary decisive functions $\mathbf{SF}$ and a subset of such functions $\mathbf{SF_i}$.

$$\{\bigcup_{i=1}^{n}\mathbf{SF_i}\}=\{\mathbf{SF_1},\ \mathbf{SF_2},\ \ldots,\ \mathbf{SF_n}\},\ (i=\overline{1,n}), \quad (14)$$

where $\mathbf{SF_i}\subseteq\mathbf{SF}$, $(i=\overline{1,n})$ will be defined as

$$\mathbf{SF_i}=\{\bigcup_{a=1}^{w_i}SF_{ia}\}=\{SF_{i1},\ SF_{i2},\ \ldots,\ SF_{iw_i}\}, \text{ a} \quad (15)$$

$$SF_{ia}=SF_{ia}(\ \mathbf{SAF_{ia}}\ ). \quad (16)$$

We should note that the function SF_{ia} defines the relationships in $\mathbf{SAF_{ia}}$, formed by the expert in the form of logical chains (based on disjunctions and conjunctions) for the subsequent construction of detection expressions, focused on identifying the i-th cyber attack.

An expert in order to obtain a specific set of binary functions that reveals a i-th cyber attack creates a corresponding template that defines relationships in $\mathbf{SAF_{ia}}$.

For example, if $\mathbf{SAF_{ia}}=\langle\ AF_{111},\ AF_{112},\ AF_{113}\ \rangle$, and the templates have the form $\langle\ AF\wedge AF\wedge AF\ \rangle$ or $\langle\ AF\wedge(AF\vee AF)\ \rangle$, then respectively $SF_{11}=AF_{111}\wedge AF_{112}\wedge AF_{113}$ or $SF_{11}=AF_{111}\wedge(AF_{112}\vee AF_{113})$.

The specific values of the elements of a subset $\mathbf{AF_i}$ $(i=\overline{1,n})$ are formed on the basis of the binary equivalence function $E(x,\ y)$, which takes the value 1 only if x and y are equal, ie,:

$$E(x,\ y)=\begin{cases}1,\ npu\ x=y\\0,\ npu\ x\neq y.\end{cases} \quad (17)$$

On the basis of this we define, that $AF_{ias}=E\ (NUM_{ia},\ s)$, and as arguments $E(x,\ y)$, we will use fuzzy terms indexes $\mathbf{T_{ij}^{ep}}$ and $\mathbf{P_i^{\tau_f p}}$.

Let consider an example of the formation of decisive functions, at $n=3$, $i=\overline{1,3}$ ($\mathbf{CA_1^{\tau_f}}=\mathbf{CA_{SN}^{\tau_f}}=\mathbf{SN^{\tau_f}}$, $\mathbf{CA_2^{\tau_f}}=\mathbf{CA_{DS}^{\tau_f}}=\mathbf{DS^{\tau_f}}$ and $\mathbf{CA_3^{\tau_f}}=\mathbf{CA_{SP}^{\tau_f}}=\mathbf{SP^{\tau_f}}$), $m_1=m_3=2$, $m_2=3$, $r_1=5$, $r_2=r_3=3$ (see the example (15) in [11]).

According to (12)

$$w_1=\prod_{j=1}^{m_1}r_j=r_1\cdot r_2=5\cdot 3=15,$$

$$w_2=\prod_{j=1}^{m_2}r_j=r_1\cdot r_2\cdot r_3=5\cdot 3\cdot 3=45,$$

$$w_3=\prod_{j=1}^{m_3}r_j=r_1\cdot r_2=5\cdot 3=15,$$

and the expression (11) will be defined as:

$$\{\bigcup_{i=1}^{3}\mathbf{AF_i}\}=\{\mathbf{AF_1},\ \mathbf{AF_2},\ \mathbf{AF_3}\}=\{\bigcup_{i=1}^{3}\{\bigtimes_{a=1}^{w_i}\mathbf{AF_{ia}}\}\}=\{\bigcup_{i=1}^{3}\{\bigtimes_{a=1}^{w_i}\{\bigcup_{s=1}^{r_j}AF_{ias}\}\}\}=$$

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

Journal of Theoretical and Applied Information Technology
31st August 2019. Vol.97. No 16

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

$$\{\{\langle \mathbf{SAF}_{11}\rangle, \langle \mathbf{SAF}_{12}\rangle, \ldots, \langle \mathbf{SAF}_{1\,15}\rangle\}, \{\langle \mathbf{SAF}_{21}\rangle, \langle \mathbf{SAF}_{22}\rangle, \ldots, \langle \mathbf{SAF}_{2\,45}\rangle\},$$
$$\{\langle \mathbf{SAF}_{31}\rangle, \langle \mathbf{SAF}_{32}\rangle, \ldots, \langle \mathbf{SAF}_{3\,15}\rangle\}\}. \quad (18)$$

In [11] there was determined that in order to detect cyber attacks SN ($\mathbf{CA}_1^{\tau_f} = \mathbf{CA}_{SN}^{\tau_f} = \mathbf{SN}^{\tau_f}$) and SP ($\mathbf{CA}_3^{\tau_f} = \mathbf{CA}_{SP}^{\tau_f} = \mathbf{SP}^{\tau_f}$), it is necessary simultaneously to use two parameters defining the 2-dimensional parametric sub-environment (NVC-AV-(КВК-ВВК)-sub-environment and NSC-NPSA-(КОП-КПОА)-sub-environment), and for a cyber attack DS ($\mathbf{CA}_2^{\tau_f} = \mathbf{CA}_{DS}^{\tau_f} = \mathbf{DS}^{\tau_f}$) – three parameters defining the 3-dimensional parametric sub-environment (NSC-SPR-DBR-(КОП-СОЗ-ЗМЗ)-sub-environment) (see (9) in [11]). And also:

NVC (КВК) – "Number of virtual channels (Количество виртуальных каналов)",

AVC (ВВК) – "Age of virtual channel (Возраст виртуального канала)",

NSC (КОП) – "Number of simultaneous connections to the server (Количество одновременных подключений к серверу)",

NPSA (КПОА) – "Number of packets with the same sender and recipient address (Количество пакетов с одинаковым адресом отправителя и получателя)",

SPR (СОЗ) – "Speed of processing requests from customers (Скорость обработки запросов от клиентов)",

DBK (ЗМЗ) – "Delay between requests from one user (Задержка между запросами от одного пользователя)".

An expert in order to obtain a specific set of functions that detect SN and SP creates a template $\langle AF \wedge AF \rangle$, and for DS – $\langle AF \wedge (AF \vee AF) \rangle$.

Further, according to the generated templates, as well as according to (15) and (18), we define, for example, $\mathbf{SF}_3$:

$$\mathbf{SF}_3 = \{\bigcup_{a=1}^{w_3} SF_{3a}\} =$$
$$\{(E(NUM_{31}, 1) \wedge E(NUM_{32}, 1)),$$
$$(E(NUM_{31}, 2) \wedge E(NUM_{32}, 1)),$$
$$(E(NUM_{31}, 3) \wedge E(NUM_{32}, 1)),$$
$$(E(NUM_{31}, 4) \wedge E(NUM_{32}, 1)),$$
$$(E(NUM_{31}, 5) \wedge E(NUM_{32}, 1))\},$$
$$\{(E(NUM_{31}, 1) \wedge E(NUM_{32}, 2)),$$
$$(E(NUM_{31}, 2) \wedge E(NUM_{32}, 2)),$$
$$(E(NUM_{31}, 3) \wedge E(NUM_{32}, 2)),$$
$$(E(NUM_{31}, 4) \wedge E(NUM_{32}, 2)),$$
$$(E(NUM_{31}, 5) \wedge E(NUM_{32}, 2))\},$$
$$\{(E(NUM_{31}, 1) \wedge E(NUM_{32}, 3)),$$
$$(E(NUM_{31}, 2) \wedge E(NUM_{32}, 3)),$$
$$(E(NUM_{31}, 3) \wedge E(NUM_{32}, 3)),$$
$$(E(NUM_{31}, 4) \wedge E(NUM_{32}, 3)),$$
$$(E(NUM_{31}, 5) \wedge E(NUM_{32}, 3))\}.$$

Figure 1 shows the expert distribution of all possible levels of anomaly generated by the attacking environment and displayed by the identifiers of the attacking actions through different values of the parameters of the NSC-NPSA-(КОП-КПОА)-sub-environment.

From the graphical interpretation (Fig. 1) it can be seen that the support blocks with the *БВН, Б* and *П* ("MORE HIGH THAN LOW", "HIGH", "LIMIT") identifiers are the most significant for identifying SN.

On the basis of this, an example of concrete calculations will be presented only for the decisive functions $(SF_{3\,11}, \ldots, SF_{3\,15})$ from $\mathbf{SF}_3$, i.e.

$$SF_{3\,11} = (E(NUM_{31}, 1) \wedge E(NUM_{32}, 3)),$$
$$SF_{3\,12} = (E(NUM_{31}, 2) \wedge E(NUM_{32}, 3)),$$
$$SF_{3\,13} = (E(NUM_{31}, 3) \wedge E(NUM_{32}, 3)),$$
$$SF_{3\,14} = (E(NUM_{31}, 4) \wedge E(NUM_{32}, 3)),$$
$$SF_{3\,15} = (E(NUM_{31}, 5) \wedge E(NUM_{32}, 3)). \quad (19)$$

Note that at $j = 1$, $r_1 = 5$, $NUM_{31} = 3$ and $s = \overline{1,5}$ for $\mathbf{T}_{31}^{e}$ (see (27) in [16])

$$\mathbf{T}_{31}^{e} = \{\bigcup_{s=1}^{5} \underset{\sim}{T}_{31s}^{ep}\} = \{\underset{\sim}{T}_{311}^{ep}, \underset{\sim}{T}_{312}^{ep}, \underset{\sim}{T}_{313}^{ep}, \underset{\sim}{T}_{314}^{ep},$$
$$\underset{\sim}{T}_{315}^{ep}\} =$$
$$\{\underset{\sim}{OM}_{31}^{ep}, \underset{\sim}{M}_{31}^{ep}, \underset{\sim}{C}_{31}^{ep}, \underset{\sim}{B}_{31}^{ep}, \underset{\sim}{OB}_{31}^{ep}\}$$

the equivalence function according to (17) takes the value

$$E(NUM_{31}, 1) = E(NUM_{31}, 2) =$$
$$E(NUM_{31}, 4) = E(NUM_{31}, 5) = 0$$

because $NUM_{31} = 3 \neq 1 \neq 2 \neq 4 \neq 5$.

This follows from the fact that $\underset{\sim}{T}_{313}^{ep} \neq \underset{\sim}{T}_{311}^{ep} \neq \underset{\sim}{T}_{312}^{ep} \neq \underset{\sim}{T}_{314}^{ep} \neq \underset{\sim}{T}_{315}^{ep}$, i.e. $\underset{\sim}{C}_{31}^{ep} \neq \underset{\sim}{OM}_{31}^{ep} \neq \underset{\sim}{M}_{31}^{ep} \neq \underset{\sim}{B}_{31}^{ep} \neq \underset{\sim}{OB}_{31}^{ep}$.

Journal of Theoretical and Applied Information Technology
31st August 2019. Vol.97. No 16

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

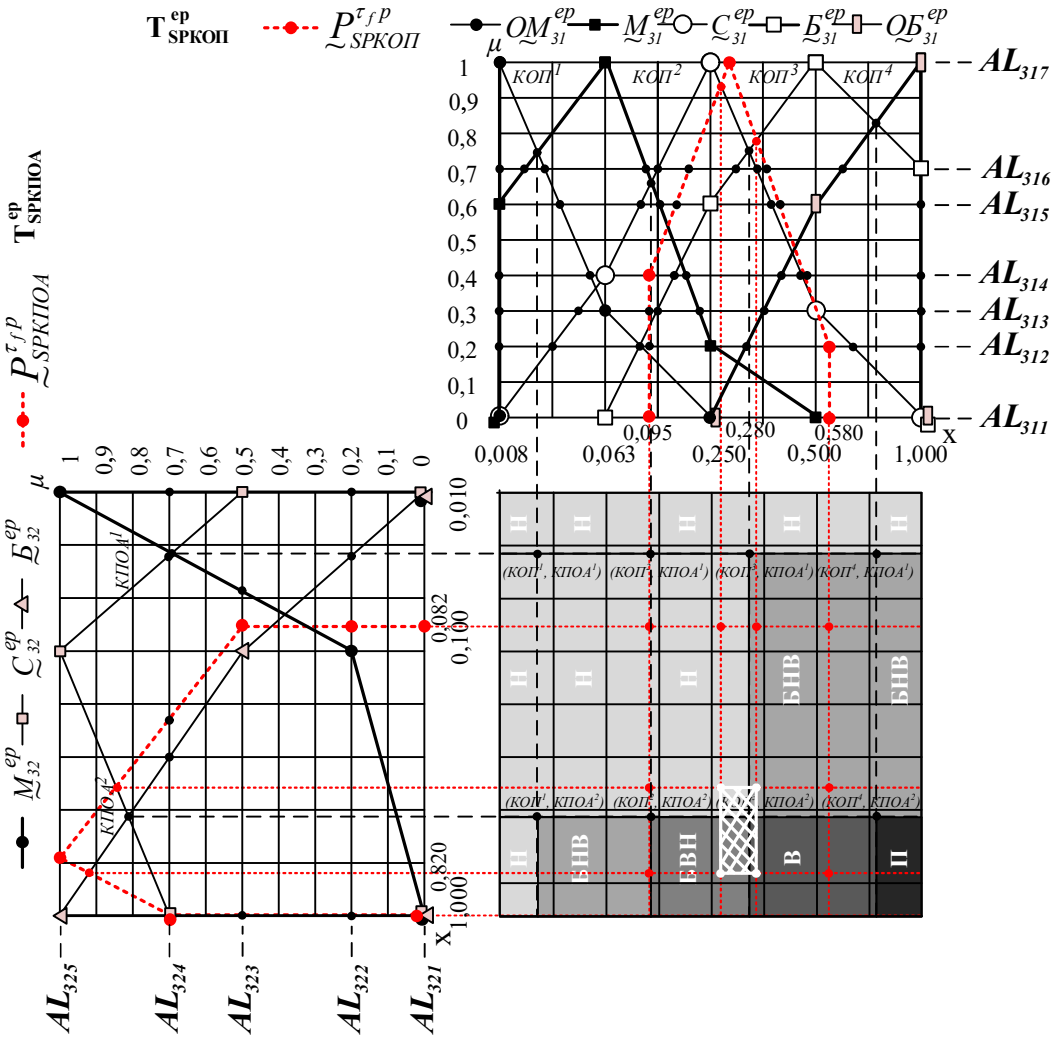

Fig. 1. Graphical interpretation of expert distribution of identifiers of attacking actions (displayed by two-dimensional support areas *Н, БНВ, БВН, В, П*)

and fuzzy values of current parameters $\underset{\sim}{P}^{\tau_f}_{31}$, $\underset{\sim}{P}^{\tau_f}_{32}$ regarding to linguistic standards $\mathbf{T}^{ep}_{31}$, $\mathbf{T}^{ep}_{32}$, respectively

Also $E(NUM_{31}, 3) = 1$ because $NUM_{31} = 3$, which follows from the fact that $\underset{\sim}{T}^{ep}_{313} = \underset{\sim}{T}^{ep}_{313}$, i.e. $\underset{\sim}{C}^{ep}_{31} = \underset{\sim}{C}^{ep}_{31}$.

Similarly for

$$\mathbf{T}^{e}_{32} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^{ep}_{32s}\} = \{\underset{\sim}{T}^{ep}_{321}, \underset{\sim}{T}^{ep}_{322}, \underset{\sim}{T}^{ep}_{323}\} =$$

$$\{\underset{\sim}{M}^{ep}_{32}, \underset{\sim}{C}^{ep}_{32}, \underset{\sim}{Б}^{ep}_{32}\}$$

at $j = 2$, $r_2 = 3$, $NUM_{32} = 3$, $s = \overline{1,3}$ (see (27) in [16]) the equivalence function according to (17) takes the value

$$E(NUM_{32}, 1) = E(NUM_{32}, 2) = 0$$

because $NUM_{32} = 3 \neq 1 \neq 2$.

This follows from the fact that $\underset{\sim}{T}^{ep}_{323} \neq \underset{\sim}{T}^{ep}_{321} \neq \underset{\sim}{T}^{ep}_{322}$, i.e. $\underset{\sim}{Б}^{ep}_{32} \neq \underset{\sim}{M}^{ep}_{32} \neq \underset{\sim}{C}^{ep}_{32}$, and $E(NUM_{32}, 3) = 1$ because $NUM_{32} = 3$, which follows from the fact that $\underset{\sim}{T}^{ep}_{323} = \underset{\sim}{T}^{ep}_{323}$, i.e. $\underset{\sim}{Б}^{ep}_{32} = \underset{\sim}{Б}^{ep}_{32}$.

Therefore

$$SF_{3\,11} = (E(NUM_{31}, 1) \wedge E(NUM_{32}, 3)) = (1 \wedge 0) = 0,$$

$$SF_{3\,12} = (E(NUM_{31}, 2) \wedge E(NUM_{32}, 3)) = (1 \wedge 0) = 0,$$

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

$$SF_{3\,13} = (E(NUM_{31}, 3) \wedge E(NUM_{32}, 3)) = (1 \wedge 1) = 1,$$

$$SF_{3\,14} = (E(NUM_{31}, 4) \wedge E(NUM_{32}, 3)) = (1 \wedge 0) = 0,$$

$$SF_{3\,15} = (E(NUM_{31}, 5) \wedge E(NUM_{32}, 3)) = (1 \wedge 0) = 0. \quad (20)$$

Stage 3 – formation of conditional detection expressions.

The conditional detection expressions that display the generated basic rules for identifying the i-th cyber attack (see (19) in [11]) can be represented in the following way:

$$\mathbf{DR_i} = \{\bigcup_{a=1}^{w_i} \mathbf{DR_{ia}}\} = \{\mathbf{DR_{i1}}, \mathbf{DR_{i2}}, \ldots, \mathbf{DR_{iw_i}}\} =$$

$$\{\mathbf{DR_{i1}} \Rightarrow \{if\ SF_{i1}\ then\ \{\bigcup_{u=1}^{v_i} IA_{iu}\}\},$$

$$\mathbf{DR_{i2}} \Rightarrow \{if\ SF_{i2}\ then\ \{\bigcup_{u=1}^{v_i} IA_{iu}\}\}, \ldots,$$

$$\mathbf{DR_{iw_i}} \Rightarrow \{if\ SF_{ia}\ then\ \{\bigcup_{u=1}^{v_i} IA_{iu}\}\}\},$$

$$(a = \overline{1, w_i},\ u = \overline{1, v_i}). \quad (21)$$

We should note that, formally, each SF_{ia} can be associated with the v_i-th amount of identifiers of the anomaly and, therefore, each basic rule can be generated by the v_i amount of detection expressions, i.e.:

$$\mathbf{DR_i} = \{\mathbf{DR_{i1}}, \mathbf{DR_{i2}}, \ldots, \mathbf{DR_{iw_i}}\} =$$

$$\{\mathbf{DR_{i1}} \Rightarrow \{if\ SF_{i1}\ then\ IA_{i1},$$

$$if\ SF_{i1}\ then\ IA_{i2}, \ldots, if\ SF_{i1}\ then\ IA_{iv_i}\},$$

$$\mathbf{DR_{i2}} \Rightarrow \{if\ SF_{i2}\ then\ IA_{i1},$$

$$if\ SF_{i2}\ then\ IA_{i2}, \ldots, if\ SF_{i2}\ then\ IA_{iv_i}\}, \ldots,$$

$$\mathbf{DR_{iw_i}} \Rightarrow \{if\ SF_{iw_i}\ then\ IA_{i1},$$

$$if\ SF_{iw_i}\ then\ IA_{i2}, \ldots, if\ SF_{iw_i}\ then\ IA_{iv_i}\}\ \text{or}$$

$$\mathbf{DR_i} = \{\bigcup_{a=1}^{w_i} \{\bigcup_{u=1}^{v_i} if\ SF_{ia}\ then\ IA_{iu}\}\},$$

$$(a = \overline{1, w_i},\ u = \overline{1, v_i}) \quad (22)$$

Obviously, the possible amount of conditional detection expressions for identifying of the i-th cyber attack is determined by the formula

$$CDR_i = w_i \cdot v_i, \quad (23)$$

and their amount to identifying of n attacks is calculated by the expression $CDR = \sum_{i=1}^{n} CDR_i$.

It should be noted that from the total amount of possible detection expressions, not all are decisive (i.e., they affect the intrusion detection process) for identifying the i-th cyber attack, which also follows from Fig. 1 and (20) (here the decisive will be $\mathbf{DR_{3\,11}} - \mathbf{DR_{3\,15}}$).

Regarding this, we consider an example of the implementation of the stage 3 at $i = 3$ ($CA_3 = CA_{SP} = SP$), $j = \overline{1,2}$ ($P_{31} = P_{SPKOII} = KOII$, $P_{32} = P_{SPKIIOA} = KIIOA$), $u_3 = 5$, $w_3 = 15$.

Then the total amount of rules is determined by the formula (23), i.e.

$$CDR_3 = w_3 \cdot v_3 = 15 \cdot 5 = 75,$$

And the expression (22) will be represented in the following way:

$$\mathbf{DR_3} = \{\ldots, \mathbf{DR_{3\,11}} \Rightarrow \{if\ SF_{3\,11}\ then\ IA_{31},$$

$$if\ SF_{3\,11}\ then\ IA_{32},\ if\ SF_{3\,11}\ then\ IA_{33},$$

$$if\ SF_{3\,11}\ then\ IA_{34},\ if\ SF_{3\,11}\ then\ IA_{35}\},$$

$$\mathbf{DR_{3\,12}} \Rightarrow \{if\ SF_{3\,12}\ then\ IA_{31},$$

$$if\ SF_{3\,12}\ then\ IA_{32},\ if\ SF_{3\,12}\ then\ IA_{33},$$

$$if\ SF_{3\,12}\ then\ IA_{34},\ if\ SF_{3\,12}\ then\ IA_{35}\},$$

$$\mathbf{DR_{3\,13}} \Rightarrow \{if\ SF_{3\,13}\ then\ IA_{31},$$

$$if\ SF_{3\,13}\ then\ IA_{32},\ if\ SF_{3\,13}\ then\ IA_{33},$$

$$if\ SF_{3\,13}\ then\ IA_{34},\ if\ SF_{3\,13}\ then\ IA_{35}\},$$

$$\mathbf{DR_{3\,14}} \Rightarrow \{if\ SF_{3\,14}\ then\ IA_{31},$$

$$if\ SF_{3\,14}\ then\ IA_{32},\ if\ SF_{3\,14}\ then\ IA_{33},$$

$$if\ SF_{3\,14}\ then\ IA_{34},\ if\ SF_{3\,14}\ then\ IA_{35}\},$$

$$\mathbf{DR_{3\,15}} \Rightarrow \{if\ SF_{3\,15}\ then\ IA_{31},$$

$$if\ SF_{3\,15}\ then\ IA_{32},\ if\ SF_{3\,15}\ then\ IA_{33},$$

$$if\ SF_{3\,15}\ then\ IA_{34},\ if\ SF_{3\,15}\ then\ IA_{35}\}\}. \quad (24)$$

According to the initial data, specified in the example, as well as taking into account the expression (20) and graphical visualization (see Fig. 1) it is clear that the decisive function is a decisive function $SF_{3\,13}$ that is included in a subset of detection expressions $\mathbf{DR_{3\,13}}$, i.e.:

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

$$\mathbf{DR}_{3\ 13} \Rightarrow \{if\ SF_{3\ 13}\ then\ IA_{31},\ if\ SF_{3\ 13}\ then\ IA_{32},\ if\ SF_{3\ 13}\ then\ IA_{33},$$
$$if\ SF_{3\ 13}\ then\ IA_{34},\ if\ SF_{3\ 13}\ then\ IA_{35}\} =$$
$$\{if\ (E(NUM_{31}, 1) \wedge E(NUM_{32}, 3))\ then\ IA_{31},$$
$$if\ (E(NUM_{31}, 2) \wedge E(NUM_{32}, 3))\ then\ IA_{32},$$
$$if\ (E(NUM_{31}, 3) \wedge E(NUM_{32}, 3))\ then\ IA_{33},$$
$$if\ (E(NUM_{31}, 4) \wedge E(NUM_{32}, 3))\ then\ IA_{34},$$
$$if\ (E(NUM_{31}, 5) \wedge E(NUM_{32}, 3))\ then\ IA_{35}\} =$$
$$\{if\ (E(NUM_{SPKOP}, 1) \wedge E(NUM_{SPKPOA}, 3))\ then\ "H",$$
$$if\ (E(NUM_{SPKOP}, 2) \wedge E(NUM_{SPKPOA}, 3))\ then\ "БНВ",$$
$$if\ (E(NUM_{SPKOP}, 3) \wedge E(NUM_{SPKPOA}, 3))\ then\ "БВН",$$
$$if\ (E(NUM_{SPKOP}, 4) \wedge E(NUM_{SPKPOA}, 3))\ then\ "В",$$
$$if\ (E(NUM_{SPKOP}, 5) \wedge E(NUM_{SPKPOA}, 3))\ then\ "П"\}.$$

After checking all the rules in $\mathbf{DR}_{3\ 13}$, we determine that the identification of the anomalous state is carried out by means of a conditional expression

$$if\ (E(NUM_{SPKOP}, 3) \wedge E(NUM_{SPKPOA}, 3))$$
$$then\ "БВН" = if\ (1 \wedge 1)\ then\ "БВН".$$

The Figure 1 graphically shows the current block (in the form of a shaded rectangular area formed by $\underset{\sim}{P}_{31}^{\tau_f}$, $\underset{\sim}{P}_{32}^{\tau_f}$) interpreting the anomaly in the 2-dimensional parametric NSC-NPSA-(КОП-КПОА)-sub-environment generated by the corresponding attacking SP-environment at the moment of time τ_f.

Here, even during visual comparing, it can be determined that the obtained current block is more closer to the fuzzy two-dimensional support area with the identifier *"БВН"* ("MORE HIGH THAN LOW"), and the used rule can literally be interpreted as: "If the current value of the fuzzy parameter "Number of simultaneous connections to the server (КОП)" at the moment of time τ_f is more closer to the standard fuzzy number "Average (Среднее – С)" and, at the same time, the current value of the fuzzy parameter "Number of packets with the same address of the sender and recipient (КПОА)" at the moment of time τ_f is more closer to the standard fuzzy number "High (Большое – Б)", then the level of the anomalous state that can be generated by the spoofing will be "More High than Low (БВН)".

Also, using the developed software for the formation of standards of parameters for cyber attack detection systems [30], using various initial data, there is created the current state area, which allows visually to assess the anomalous state in the system in order to make the necessary decision. Here, the current block is generated, for example, in the form of a red rectangular area formed by $\underset{\sim}{P}_{31}^{\tau_f}$ and $\underset{\sim}{P}_{32}^{\tau_f}$, which interprets the anomaly in the 2-dimensional parametric NSC-NPSA--(КОП-КПОА)-sub-environment generated by the corresponding attacking SP-environment at the moment of time τ_f [11].

An example of the work of software for the formation of standards of parameters with different input data is shown on Fig. 2.

This software allows to automate the process of formation of standards of parameters for modern systems of anomaly detection and to display the results of the detection of an anomalous state in a given period of time τ_f.

Similarly, with different initial data there are identified other types of cyber attacks, generating certain anomalies in information systems.

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

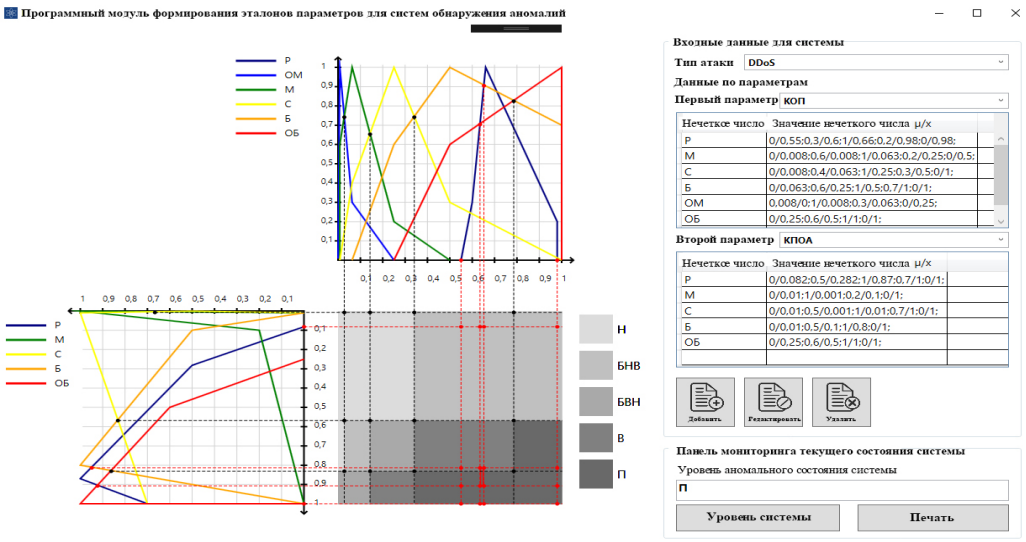

Fig. 2. Example of the work of software for the formation of standards of parameters (Determination of the current state of the system)

5. CONCLUSIONS

Therefore, in the work there was proposed the DEFM, which on the basis of the basic tuple model [11], using the mechanism of formation the subsets of anomaly identifiers, formalizing the process of creation of decisive functions and conditional detection expressions, allows to form the necessary set of detection rules used to determine the level of anomalous state which is characteristic to a certain type of attacks. The use of this method at the creation anomaly detection systems will expand their functionality regarding to the detection of cyber attacks in a weakly formalized fuzzy environment.

REFERENCES

[1]. Mohammad Almseidin, Szilveszter Kovacs, «Intrusion detection mechanism using fuzzy rule interpolation», Journal of Theoretical and Applied Information Technology, vol. 96, no. 16, pp. 5473-5488, 2018.

[2]. 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.

[3]. 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.

[4]. 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.

[5]. 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.

[6]. 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.

[7]. 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.

[8]. 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.

[9]. 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.

[10]. Mohammed Ali Tawfiq «Security Measurements of Internet Website Zone for IE9 Based on Fuzzy Logic» Journal of

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

Engineering and Development. Vol. 17, № 1, Mar. 2013, pp. 255-269.

[11]. 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)

[12]. 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.

[13]. 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.

[14]. Akhmetov, B., Kydyralina L, Lakhno V., Mohylnyi G., AkhmetovaJ., Tashimova A., model for a computer decision support system on mutual investment in the cybersecurity of educational institutions //International Journal of Mechanical Engineering and Technology (IJMET)//, Volume 9, Issue 10, October 2018, pp. 1114–1122,

[15]. A. Korchenko, K. Warwas, A. Kłos-Witkowska, «The Tupel Model of Basic Components' Set Formation for Cyberattacks», in Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2015 IEEE 8th International Conference on, 2015, pp. 478-483.

[16]. Korchenko A.A. The formation method of linguistic standards created for the intrusion detection systems, Zahist ìnformacìï, vol. 16, №1, 2014, pp. 5-12. (in Russian)

[17]. B. Akhemetov, A. Korchenko, S. Akhmetova, N. Zhumangalieva, «Improved method for the formation of linguistic standards for of intrusion detection systems», Journal of Theoretical and Applied Information Technology, vol. 87, no. 2, pp. 221-232, 2016.

[18]. Tereykovsky I., Korchenko A., Vikulov P., Shakhoval O., The etalons models of linguistic variables for sniffing attacks detection, Zahist ìnformacìï, vol. 19, №3, 2017, pp. 228-242. (in Russian)

[19]. Mikolaj Karpinski, Poland, Anna Korchenko, Pavlo Vikulov, Ukraine, Roman Kochan. The Etalon Models of Linguistic Variables for Sniffing-Attack Detection // Proceedings of the 2017 IEEE 9th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2017), Romania, Bucharest, September 21-23, 2017: Vol. 1. – Pp. 258-264.

[20]. Tereykovsky I., Korchenko A., Vikulov P., Ireifidzh I., Etalons models of linguistic variables for email-spoofing-attack detection systems, Bezpeka ìnformacìï, vol. 24 №2, pp. 21-28, 2018. (in Russian)

[21]. Korchenko A. Method of parameter fuzzification based on linguistic standards for cyber attacks detection, Bezpeka ìnformacìï, 2014, vol. 20, issue 1, pp. 21-28. (in Russian)

[22]. Korchenko A., The method of α-level of nominalization for intrusion detection systems, Zahist ìnformacìï, vol. 16, №4, 2014, pp. 292-304. (in Russian)

[23]. Korchenko A.O. The detection method of identification terms for intrusion detection system, Bezpeka ìnformacìï, 2014, Vol.20, №3, pp. 217-223. (in Russian)

[24]. Tereykovsky I., Korchenko A., «Cyber attack detection system», Bezpeka ìnformacìï, 2017, Vol.23, №3, pp. 176-180. (in Russian)

[25]. Deep neural networks in cyber attack detection systems / Bapiyev, I.M., Aitchanov, B.H., Tereikovskyi, I.A., Tereikovska, L.A., Korchenko, A.A. // International Journal of Civil Engineering and Technology Vol. 8, Issue 11, November 2017, PP. 1086-1092.

[26]. Lakhno, V., Akhmetov, B., Korchenko, A., Alimseitova, Z., Grebenuk, V., Development of a decision support system based on expert evaluation for the situation center of transport cybersecurity, Journal of Theoretical and Applied Information Technology, 2018, 96(14), c. 4530-4540.

[27]. Borowik B., Borowik Barbara, Karpinskyi V., Klos–Witkowska A., Shaikhanova A. (2018, July). Wind turbine model with PIC microcontroller power control. In 2018 18th International Multidisciplinary Scientific Conference (SCEM2018). Vol. 18, Issue 4.1, pp. 823-830

[28]. Belginova, S., Uvaliyeva, I., & Ismukhamedova, A. (2018, May). Decision support system for diagnosing anemia. In 2018 4th International Conference on Computer and Technology Applications (ICCTA) (pp. 211-215).

[29]. 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)

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

[30]. Korchenko A, Zaritskyi O., Taras P., Bychkov V., The software for the formation of parameters etalons for cyber-attacks detection systems, Zahist ìnformacìï, vol.20, №3, 2018, pp. 133-148. (in Russian)