УДК 004.056.53(045)

МЕТОД ФОРМИРОВАНИЯ ЛИНГВИСТИЧЕСКИХ ЭТАЛОНОВ ДЛЯ СИСТЕМ ВЫЯВЛЕНИЯ ВТОРЖЕНИЙ

Анна Корченко

Одним из решений обеспечения информационной безопасности являются системы выявления вторжений, основанные на аномальном принципе. Для построения такого рода систем используется метод выявления аномалий, порожденных кибератаками в информационных системах. В этом методе процесс формирования различных эталонов достаточно трудоемкий и практически не формализован, что понижает эффективность его использования. С целью компенсации этого недостатка предлагается метод, который базируется на математических моделях и методах нечеткой логики и реализуется посредством шести базовых этапов: формирование подмножеств идентификаторов лингвистических оценок, формирование базовой матрицы частот, формирование производной матрицы частот, формирование нечетких термов, формирование эталонных нечетких чисел, визуализация лингвистических эталонов. Метод позволяет усовершенствовать процесс формализации получения лингвистических эталонов параметров для повышения эффективности построения соответствующих систем выявления вторжений.

Ключевые слова: *кибератаки, аномалии, нечеткие эталоны, метод формирования лингвистических эталонов, системы обнаружения вторжений, системы обнаружения аномалий, системы обнаружения атак, обнаружение аномалий в компьютерных сетях.*

В стремительно развивающемся киберпространстве появляются новые виды угроз его ресурсам. В этой связи существует потребность в системах кибербезопасности, позволяющих анализировать, контролировать, прогнозировать и блокировать новые виды кибератак на информационные системы. Для этого необходимы средства, дающие возможность идентифицировать вторжения, порождающие аномалии в определенной среде окружения. Достаточно эффективными средствами безопасности являются системы [1-3], используемые для выявления вторжений, основанные на идентификации в нечетких условиях аномального состояния по заданному набору параметров, характерных для конкретной среды окружения. Для построения такого рода систем используется метод выявления аномалий, порожденных кибератаками в информационных системах [4]. В этом методе процесс формирования различных эталонов достаточно трудоемкий и практически не формализован, что понижает эффективность его использования. Исходя из этого, создание методов, позволяющих усовершенствовать процесс формализации получения лингвистических эталонов параметров для систем выявления вторжений, есть актуальной задачей.

В связи с этим, целью данной работы является разработка обобщенного метода формирования лингвистических эталонов (МФЛЭ), позволяющего формализовать процесс получения эталонов параметров для заданных групп лингвистических переменных конкретной среды окружения при решении задач выявления атак в компьютерных системах. Обобщенный МФЛЭ частично основывается на МЛТС [5] и представляется в виде шести этапов.

Этап 1 – формирование подмножеств идентификаторов лингвистических оценок. Для реализации этого этапа вводится множество всех возможных идентификаторов лингвистических оценок (суждений) эксперта **LE** и подмножества таких идентификаторов $\mathbf{LE_{ij}} \in \mathbf{LE}$, которые отображают используемые им суждения для характеристики текущего состояния *j*-го параметра относительно *i*-й атаки при его наблюдении в определенной среде окружения. Таким образом, относительно *j*-го параметра эксперт может применить набор из r высказываний (лингвистических оценок), отображаемый подмножеством

$$\mathbf{LE_{ij}} = \bigcup_{k=1}^{r} \mathrm{LE}_{ijk} = \{LE_{ij1},\ LE_{ij2},\ \ldots,\ LE_{ijk},\ \ldots,\ LE_{ijr}\}, \quad (1)$$

где LE_{ijk} $(k = \overline{1,r})$ – идентификатор лингвистической оценки эксперта относительно состояния *j*-го параметра при *i*-й атаке.

Например, для реализации лингвистической оценки эксперта при $i = 2$, $j = 3$ (т.е. AT_2=*DS* – «Отказ в обслуживании (DoS)», P_3=*КОП* – «Количество одновременных подключений к серверу» [6]) и $r = 5$ подмножество $\mathbf{LE_{ij}}$=$\mathbf{LE_{23}}$ согласно выражению (1) принимает вид

$$\mathbf{LE_{23}} = \bigcup_{k=1}^{5} LE_{23k} = \{ LE_{231},\ LE_{232},\ \ldots,$$

$$LE_{235} \} = \{ LE_{DSKOП1},\ LE_{DSKOП2},\ \ldots,\ LE_{DSKOП5} \} =$$

$$\{ "ОМ", "М", "С", "Б", "ОБ" \},$$

где $LE_{\text{DS КОП1}} = "ОМ"$, $LE_{\text{DS КОП2}} = "М"$, $LE_{\text{DS КОП3}} = "С"$, $LE_{\text{DS КОП4}} = "Б"$ и $LE_{\text{DS КОП5}} = "ОБ"$ соответственно отображают оценку эксперта: «ОЧЕНЬ МАЛОЕ» ("ОМ"), «МАЛОЕ» ("М"), «СРЕДНЕЕ» ("С"), «БОЛЬШОЕ» ("Б") и «ОЧЕНЬ БОЛЬШОЕ» ("ОБ").

Этап 2 – формирование базовой матрицы частот. Для получения такой матрицы вводится множество идентификаторов интервалов $\mathbf{N}$ и подмножества таких идентификаторов $\mathbf{N}_{ij} \in \mathbf{N}$, которые отображаются как

$$\mathbf{N}_{ij} = \bigcup_{k=1}^{r} \mathrm{N}_{ijk} = \{N_{ij1},\ N_{ij2},\ \ldots,\ N_{ijk},\ \ldots,\ N_{ijr}\}, \qquad (2)$$

где N_{ijk} $(k = \overline{1,r})$ – идентификатор k-го интервала, используемого для формирования на нем частот встречаемости оценок эксперта по текущему состоянию j-го параметра относительно i-й атаки, а r – количество идентификаторов фиксированных интервалов, на которых осуществляется указанная оценка.

На основе элементов подмножеств $\mathbf{LE}_{ij}$ и $\mathbf{N}_{ij}$ формируется обобщенная таблица оценок (табл. 1), содержимое которой основывается на текущем фиксировании свидетельств (суждений, оценок) эксперта, где f_{ijsq} $(s,q = \overline{1,r})$ – элементы эмпирических данных, отображающие количество (частоту) одинаковых высказываний (использования лингвистической оценки из подмножества $\mathbf{LE}_{ij}$) эксперта, характеризующих состояние j-го параметра на интервале с идентификатором $N_{ijq} \stackrel{\text{def}}{=} [N_{ijq}^{min}; N_{ijq}^{max}]$ $(q = \overline{1,r})$, где N_{ijq}^{min} и N_{ijq}^{max} соответственно нижняя и верхняя граница q-го интервала.

Таблица 1

Обобщенная таблица оценок по $\mathbf{LE}_{ij}$

$\mathbf{LE}_{ij}$	$\mathbf{N}_{ij}$					
	N_{ij1}	N_{ij2}	…	N_{ijq}	…	N_{ijr}
LE_{ij1}	f_{ij11}	f_{ij12}	…	f_{ij1q}	…	f_{ij1r}
LE_{ij2}	f_{ij21}	f_{ij22}	…	f_{ij2q}	…	f_{ij2r}
…	…	…	…	…	…	…
LE_{ijs}	f_{ijs1}	f_{ijs2}	…	f_{ijsq}	…	f_{ijsr}
…	…	…	…	…	…	…
LE_{ijr}	f_{ijr1}	f_{ijr2}	…	f_{ijrq}	…	f_{ijrr}

Далее на основе обобщенной таблицы оценок по элементам подмножества $\mathbf{LE}_{ij}$ (см. табл. 1) формируется базовая матрица частот

$$F_{ij} = \left\| f_{ijsq} \right\| = \underset{(s,q=\overline{1,r})}{\begin{vmatrix} f_{ij11} & f_{ij12} & \cdots & f_{ij1q} & \cdots & f_{ij1r} \\ f_{ij21} & f_{ij22} & \cdots & f_{ij2q} & \cdots & f_{ij2r} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ f_{ijs1} & f_{ijs2} & \cdots & f_{ijsq} & \cdots & f_{ijsr} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ f_{ijr1} & f_{ijr2} & \cdots & f_{ijrq} & \cdots & f_{ijrr} \end{vmatrix}}. \qquad (3)$$

Например, если требуется сформировать матрицу F_{ij} при $i = 2$, $j = 3$ (т.е. AT_2=DS, P_3=$КОП$) и $r = 5$, то

$$\mathbf{N}_{23} = \bigcup_{k=1}^{5} N_{23k} = \{N_{231},\ N_{232},\ \ldots,\ N_{235}\} <=>$$

$$\mathbf{N}_{\mathbf{DSКОП}} = \bigcup_{k=1}^{5} N_{DSКОПk} = \{N_{DSКОП1},\ N_{DSКОП2},\ N_{DSКОП3},\ N_{DSКОП4},\ N_{DSКОП5}\}.$$

На основе обобщенной таблицы (см. табл. 1) построим текущую таблицу оценок (табл. 2) по элементам подмножества $LE_{ijk} = LE_{23k} = LE_{\text{DS КОПk}}$ $(k = \overline{1,5})$, где $LE_{231} = LE_{\text{DS КОП1}} = "ОМ"$, $LE_{232} = LE_{\text{DS КОП2}} = "М"$, $LE_{233} = LE_{\text{DS КОП3}} = "С"$, $LE_{234} = LE_{\text{DS КОП4}} = "Б"$, $LE_{235} = LE_{\text{DS КОП5}} = "ОБ"$ и $N_{ijk} = N_{23k} = N_{\text{DS КОПk}}$, а $N_{ij1} = N_{\text{DS КОП1}} \stackrel{\text{def}}{=} [N_{\text{DS КОП1}}^{\min}; N_{\text{DS КОП1}}^{\max}] <=> [0; 8]$, $N_{ij2} = N_{\text{DS КОП2}} \stackrel{\text{def}}{=} [N_{\text{DS КОП2}}^{\min}; N_{\text{DS КОП2}}^{\max}] <=> [9; 64]$, $N_{ij3} = N_{\text{DS КОП3}} \stackrel{\text{def}}{=} [N_{\text{DS КОП3}}^{\min}; N_{\text{DS КОП3}}^{\max}] <=> [65; 256]$, $N_{ij4} = N_{\text{DS КОП4}} \stackrel{\text{def}}{=} [N_{\text{DS КОП4}}^{\min}; N_{\text{DS КОП4}}^{\max}] <=> [257; 512]$ и $N_{ij5} = N_{\text{DS КОП5}} \stackrel{\text{def}}{=} [N_{\text{DS КОП5}}^{\min}; N_{\text{DS КОП5}}^{\max}] <=> [513; 1024]$.

Таблица 2

Текущая таблица оценок по $\mathbf{LE_{23}}$

$\mathbf{LE_{23}}$= $\mathbf{LE_{DSКОП}}$	$\mathbf{N_{23}}$=$\mathbf{N_{DSКОП}}$				
	$N_{\text{DS КОП1}}$	$N_{\text{DS КОП2}}$	$N_{\text{DS КОП3}}$	$N_{\text{DS КОП4}}$	$N_{\text{DS КОП5}}$
"ОМ"	4	1	0	0	0
"М"	2	3	1	0	0
"С"	0	1	4	2	0
"Б"	0	0	2	4	3
"ОБ"	0	0	0	5	6

Далее, при $s,q = \overline{1,5}$ согласно выражения (3) с использованием данных табл. 2 сформируем матрицу частот, т.е.

$$F_{23} = F_{DSКОП} = \left\| f_{23sq} \right\| = \left\| f_{DSКОПsq} \right\| =$$

$$\begin{Vmatrix} f_{2311} & f_{2312} & f_{2313} & f_{2314} & f_{2315} \\ f_{2321} & f_{2322} & f_{2323} & f_{2324} & f_{2325} \\ f_{2331} & f_{2332} & f_{2333} & f_{2334} & f_{2335} \\ f_{2341} & f_{2342} & f_{2343} & f_{2344} & f_{2345} \\ f_{2351} & f_{2352} & f_{2353} & f_{2354} & f_{2355} \end{Vmatrix} = \begin{Vmatrix} 4 & 1 & 0 & 0 & 0 \\ 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 4 & 2 & 0 \\ 0 & 0 & 2 & 4 & 3 \\ 0 & 0 & 0 & 5 & 6 \end{Vmatrix}.$$

Этап 3 – формирование производной матрицы частот. Для реализации этого этапа создается вектор сумм (VS_{ij}) по соответствующим столбцам матрицы частот (3), т.е.

$$\begin{aligned} \mathrm{VS_{ij}} &= \left\|vs_{ijq}\right\| = \left\|vs_{ij1}, vs_{ij2}, ..., vs_{ijq}, ..., vs_{ijr}\right\| = \\ &\left\|\sum_{s=1}^{r} f_{ijs1}, \sum_{s=1}^{r} f_{ijs2}, ..., \sum_{s=1}^{r} f_{ijsq}, ..., \sum_{s=1}^{r} f_{ijsr}\right\| = \\ &\left\|\bigcup_{q=1}^{r}\sum_{s=1}^{r} f_{ijsq}\right\| \ (q=\overline{1,r}), \end{aligned} \tag{4}$$

где f_{ijsq} – элементы матрицы F_{ij}. Далее из членов VS_{ij} определяем максимальное значение по формуле

$$\mathrm{vsm_{ij}} = \bigvee_{q=1}^{\mathrm{r}} vs_{ijq}, \tag{5}$$

которое используется для формирования производной матрицы частот

$$F_{ij}^{'} = \left\|f_{ijsq}^{'}\right\| = (vsm_{ij}/vs_{ijq})\left\|f_{ijsq}\right\| <=>$$

$$F_{ij}^{'} = (\mathrm{vsm_{ij}}/vs_{ijq})\mathrm{F_{ij}} = \begin{Vmatrix} f_{ij11}^{'} & f_{ij12}^{'} \cdots f_{ij1q}^{'} \cdots f_{ij1r}^{'} \\ f_{ij21}^{'} & f_{ij22}^{'} \cdots f_{ij2q}^{'} \cdots f_{ij2r}^{'} \\ \cdots \ \cdots \ \cdots \ \cdots \ \cdots \ \cdots \\ f_{ijs1}^{'} & f_{ijs2}^{'} \cdots f_{ijsq}^{'} \cdots f_{ijsr}^{'} \\ \cdots \ \cdots \ \cdots \ \cdots \ \cdots \ \cdots \\ f_{ijr1}^{'} & f_{ijr2}^{'} \cdots f_{ijrq}^{'} \cdots f_{ijrr}^{'} \end{Vmatrix}. \tag{6}$$

Рассмотрим формирование $F_{ij}^{'}$ на конкретном примере. Для этого при $i=2$, $j=3$ создадим вектор сумм $\mathrm{VS_{ij}} = \mathrm{VS_{23}}$ по соответствующим столбцам матрицы частот (3) с использованием выражения (4), т.е.

$$\mathrm{VS_{23}} = \left\|vs_{23q}\right\| = \left\|vs_{231}, vs_{232}, vs_{233}, vs_{234}, vs_{235}\right\| =$$

$$\left\|\bigcup_{q=1}^{5}\sum_{s=1}^{5} \mathrm{f_{23sq}}\right\| <=> \mathrm{VS_{DS\,KOП}} = \left\|vs_{\mathrm{DS\,KOП}q}\right\| =$$

$$\left\|vs_{\mathrm{DSKOП1}}, vs_{\mathrm{DSKOП2}}, vs_{\mathrm{DSKOП3}}, vs_{\mathrm{DSKOП4}}, vs_{\mathrm{DSKOП5}}\right\| =$$

$$\left\|\bigcup_{q=1}^{5}\sum_{s=1}^{5} \mathrm{f_{DSKOПsq}}\right\| = \left\|6, 5, 7, 11, 9\right\| \ (q=\overline{1,5}).$$ Далее из $\mathrm{VS_{23}} = \mathrm{VS_{DSKOП}}$ по формуле (5) определяем максимальный элемент $\mathrm{vsm_{23}} = \bigvee_{q=1}^{5} vs_{23q} = \mathrm{vs_{231}} \vee \mathrm{vs_{232}} \vee \mathrm{vs_{233}} \vee \mathrm{vs_{234}} \vee \mathrm{vs_{235}} = 6 \vee 5 \vee 7 \vee 11 \vee 9 = \mathrm{vsm_{DS\,KOП}} = 11$, а производную матрицу частот $F_{23}^{'} = \left\|\mathrm{f_{23sq}^{'}}\right\| = (\mathrm{vsm_{23}}/vs_{23q})\left\|\mathrm{f_{23sq}}\right\| = F_{\mathrm{DS\,KOП}}^{'}$ получим согласно выражения (6)

$$F_{DSKOП}^{'} = (vsm_{DSKOП}/vs_{DSKOП\,q})F_{DSKOП} = \begin{Vmatrix} 7{,}33 & 2{,}2 & 0 & 0 & 0 \\ 3{,}66 & 6{,}6 & 1{,}57 & 0 & 0 \\ 0 & 2{,}2 & 6{,}29 & 2 & 0 \\ 0 & 0 & 3{,}14 & 4 & 3{,}66 \\ 0 & 0 & 0 & 5 & 7{,}33 \end{Vmatrix}.$$

Этап 4 – формирование нечетких термов. Для реализации этого этапа согласно выражения (7) строится вектор максимумов по соответствующим строкам $F_{ij}^{'}$, т.е.:

$$\begin{aligned} FM_{ij} &= \\ \left\|fm_{ijq}\right\| &= \left\|fm_{ij1}, fm_{ij2}, ..., fm_{ijq}, ..., fm_{ijr}\right\| = \\ &\left\|\bigvee_{s=1}^{r} f_{ijs1}^{'}, \bigvee_{s=1}^{r} f_{ijs2}^{'}, ..., \bigvee_{s=1}^{r} f_{ijsq}^{'}, ..., \bigvee_{s=1}^{r} f_{ijsr}^{'}\right\| = \\ &\left\|\bigcup_{q=1}^{r}\bigvee_{s=1}^{r} f_{ijsq}^{'}\right\| \ (q=\overline{1,r}). \end{aligned} \tag{7}$$

На основании FM_{ij} сформируем матрицу функций принадлежности

$$M_{ij} = \left\|\mu_{ijsq}\right\| = \begin{Vmatrix} \mu_{ij11} & \mu_{ij12} \cdots \mu_{ij1q} \cdots \mu_{ij1r} \\ \mu_{ij21} & \mu_{ij22} \cdots \mu_{ij2q} \cdots \mu_{ij2r} \\ \cdots \ \cdots \ \cdots \ \cdots \ \cdots \ \cdots \\ \mu_{ijs1} & \mu_{ijs2} \cdots \mu_{ijsq} \cdots \mu_{ijsr} \\ \cdots \ \cdots \ \cdots \ \cdots \ \cdots \ \cdots \\ \mu_{ijr1} & \mu_{ijr2} \cdots \mu_{ijrq} \cdots \mu_{ijrr} \end{Vmatrix}, \tag{8}$$

каждый элемент которой вычисляется по выражению $\mu_{ijsq} = f_{ijsq}^{'}/fm_{ijs} \ \ (s,q=\overline{1,r})$. Используя формулу (8), определим наборы нечетких термов (чисел) $\underset{\sim}{T}_{ijs}$ на основе выражения

$$\begin{aligned} \underset{\sim}{T}_{ijs} = \{\bigcup_{q=1}^{r} \mu_{\mathrm{ijsq}} / x_{ijsq}\} = \{&\mu_{\mathrm{ijs1}} / x_{ijs1}, \mu_{\mathrm{ijs2}} / x_{ijs2}, ..., \\ &\mu_{\mathrm{ijsq}} / x_{ijsq}, ..., \mu_{\mathrm{ijsr}} / x_{ijsr}\} \ (\mathrm{q}=\overline{1,\mathrm{r}}), \end{aligned} \tag{9}$$

где $x_{ijsq} = N_{ijq}^{max}/N_{ijr}^{max} \ \ (q=\overline{1,r})$. (10)

Таким образом, нечеткие числа (НЧ) $\underset{\sim}{T}_{ijs}$ $(s=\overline{1,\mathrm{r}})$ являются интерпретацией лингвистичес-

ких высказываний экспертов, отображаемых элементами подмножества $\mathbf{LE_{ij}} \in \mathbf{LE}$ и определяются относительно *j*-го параметра *i*-й атаки как подмножества нечетких термов

$$\mathbf{T_{ij}} = \bigcup_{s=1}^{r} \underset{\sim}{T}_{ijs} = \{\underset{\sim}{T}_{ij1}, \underset{\sim}{T}_{ij2}, \ldots, \underset{\sim}{T}_{ijs}, \ldots, \underset{\sim}{T}_{ijr}\} \ (\mathbf{T_{ij}} \in \mathbf{T}), \quad (11)$$

входящих в $\mathbf{T}$ – множество всех возможных нечетких термов, используемых для идентификации кибератак.

Покажем процесс формирования Tij на конкретном примере. Пусть $i = 2$, $j = 3$ и $s = \overline{1, 5}$, тогда на основе выражения (7) построим вектор максимумов по соответствующим строкам $F'_{23} = F'_{DSKOП}$ т.е. $FM_{DSKOП} = \|fm_{DSKOПs}\| = \|fm_{DSKOП1}, fm_{DSKOП2}, fm_{DSKOП3}, fm_{DSKOП4}, fm_{DSKOП5}\| = \|7{,}33;\ 6{,}6;\ 6{,}29;\ 4;\ 7{,}33\|$.

На основании $FM_{DSKOП}$ по выражению (8) сформируем матрицу функций принадлежности $M_{DSKOП}$ получив таким образом:

$$M_{DSKOП} = \|\mu_{DSKOПsq}\| = \begin{Vmatrix} 1 & 0{,}3 & 0 & 0 & 0 \\ 0{,}55 & 1 & 0{,}24 & 0 & 0 \\ 0 & 0{,}35 & 1 & 0{,}32 & 0 \\ 0 & 0 & 0{,}8 & 1 & 0{,}9 \\ 0 & 0 & 0 & 0{,}68 & 1 \end{Vmatrix},$$

где $\mu_{DSKOПsq} = f'_{DSKOПsq} / fm_{DSKOПs}$ $(s, q = \overline{1, 5})$. На основе вычисленных по выражению (8) $\mu_{DSKOПsq}$ и выражению (10) $x_{DSKOПsq}$ определим наборы нечетких термов $\underset{\sim}{T}_{DSKOП}$ по формуле (9), т.е. $\underset{\sim}{T}_{23_s} = \{\mu_{23s1} / x_{23s1}, \mu_{23s2} / x_{23s2}, \mu_{23s3} / x_{23s3}, \mu_{23s4} / x_{23s4}, \mu_{23s5} / x_{23s5}\} <=> \underset{\sim}{T}_{DSKOП_s} = \{\mu_{DSKOПs1} / x_{DSKOПs1}, \mu_{DSKOПs2} / x_{DSKOПs2}, \mu_{DSKOПs3} / x_{DSKOПs3}, \mu_{DSKOПs4} / x_{DSKOПs4}, \mu_{DSKOПs5} / x_{DSKOПs5}\}$ $(s = \overline{1,5})$, где согласно выражения (10) $x_{DSKOПsq} = N^{max}_{DSKOПq} / N^{max}_{DSKOПr}$ $(q = \overline{1,5})$ или $\{\bigcup_{q=1}^{5} x_{DSKOПsq}\} = \{0{,}008;\ 0{,}063;\ 0{,}25;\ 0{,}5;\ 1\}$.

По выражению (11) при $i = 2$, $j = 3$ (т.е. AT_2=*DS*, P_3=*КОП*) сформируем $\mathbf{T_{23}} \in \mathbf{T}$, т.е.

$$\mathbf{T_{23}} = \bigcup_{s=1}^{5} \underset{\sim}{T}_{23s} = \{\underset{\sim}{T}_{231}, \underset{\sim}{T}_{232}, \underset{\sim}{T}_{233}, \underset{\sim}{T}_{234}, \underset{\sim}{T}_{235}\} =$$

$$\{\underset{\sim}{T}_{DSKOП1}, \underset{\sim}{T}_{DSKOП2}, \underset{\sim}{T}_{DSKOП3}, \underset{\sim}{T}_{DSKOП4}, \underset{\sim}{T}_{DSKOП5}\} = \{\underset{\sim}{QM}_{23}, \underset{\sim}{M}_{23}, \underset{\sim}{C}_{23}, \underset{\sim}{Б}_{23}, \underset{\sim}{QБ}_{23}\}$$

$(s = \overline{1,5})$, где $\underset{\sim}{T}_{231} = \underset{\sim}{T}_{DSKOП1} = \underset{\sim}{QM}_{23}$, $\underset{\sim}{T}_{232} = \underset{\sim}{T}_{DSKOП2} = \underset{\sim}{M}_{23}$, $\underset{\sim}{T}_{233} = \underset{\sim}{T}_{DSKOП3} = \underset{\sim}{C}_{23}$, $\underset{\sim}{T}_{234} = \underset{\sim}{T}_{DSKOП4} = \underset{\sim}{Б}_{23}$ и $\underset{\sim}{T}_{235} = \underset{\sim}{T}_{DSKOП5} = \underset{\sim}{QБ}_{23}$ соответственно являются НЧ $\underset{\sim}{QM}_{23}$, $\underset{\sim}{M}_{23}$, $\underset{\sim}{C}_{23}$, $\underset{\sim}{Б}_{23}$ и $\underset{\sim}{QБ}_{23}$, интерпретирующие высказывания эксперта, отображаемые посредством $LE_{DSKOП1} = "QM"$, $LE_{DSKOП2} = "M"$, $LE_{DSKOП3} = "C"$, $LE_{DSKOП4} = "Б"$ и $LE_{DSKOП5} = "QБ"$.

Таким образом, полученные члены подмножества $\mathbf{T_{23}}$ (числовая форма) соответственно являются отображением членов подмножества $\mathbf{LE_{23}}$ (лингвистическая форма) и представляются в следующем виде: $\underset{\sim}{T}_{231} = \underset{\sim}{T}_{DSKOП1} = \underset{\sim}{QM}_{23} = \{1/0{,}008;\ 0{,}3/0{,}063;\ 0/0{,}25;\ 0/0{,}5;\ 0/1\}$, $\underset{\sim}{T}_{232} = \underset{\sim}{T}_{DSKOП2} = \underset{\sim}{M}_{23} = \{0{,}55/0{,}008\ ;\ 1/0{,}063;\ 0{,}24/0{,}25;\ 0/0{,}5;\ 0/1\}$, $\underset{\sim}{T}_{233} = \underset{\sim}{T}_{DSKOП3} = \underset{\sim}{C}_{23} = \{0/0{,}008;\ 0{,}35/0{,}063;\ 1/0{,}25;\ 0{,}32\ /0{,}5;\ 0/1\}$, $\underset{\sim}{T}_{234} = \underset{\sim}{T}_{DSKOП4} = \underset{\sim}{Б}_{23} = \{0/0{,}008;\ 0/0{,}063;\ 0{,}8/0{,}25;\ 1/0{,}5;\ 0{,}9/1\}$, $\underset{\sim}{T}_{235} = \underset{\sim}{T}_{DSKOП5} = \underset{\sim}{QБ}_{23} = \{0/0{,}008;\ 0/0{,}063;\ 0/0{,}25;\ 0{,}68/0{,}5;\ 1/1\}$.

Этап 5 – формирование эталонных НЧ. Для реализации этого этапа введем множество $\mathbf{T^e}$ всех возможных нечетких (лингвистических) эталонов, используемых для идентификации кибератак и подмножества таких эталонов $\mathbf{T^e_{ij}} \in \mathbf{T^e}$, каждое из которых отображает возможные базовые состояния *j*-го параметра относительно *i*-й атаки, строится на суждениях экспертов, идентифицируемых $\mathbf{LE_{ij}}$ и определяется как

$$\mathbf{T^e_{ij}} = \bigcup_{s=1}^{r} \underset{\sim}{T}^e_{ijs} = \{\underset{\sim}{T}^e_{ij1}, \underset{\sim}{T}^e_{ij2}, \ldots, \underset{\sim}{T}^e_{ijs}, \ldots, \underset{\sim}{T}^e_{ijr}\}, \quad (12)$$

где $\underset{\sim}{T}^e_{ijs}$ $(s = \overline{1,r})$ – эталонные НЧ. Формирование нечетких эталонов основывается на преобразовании соответствующих НЧ (9) из подмножества $\mathbf{T_{ij}} \in \mathbf{T}$ и реализуется посредством трех шагов.

Шаг 1. Преобразование нечетких термов (9) таким образом, чтобы для всех $\underset{\sim}{T}_{ijs}$ было справедливо отношение порядка, т.е. $\forall x_{ijsq}: x_{ijsq} < x_{ijsq+1}$ $(q = \overline{1, r-1})$.

Шаг 2. В каждом $\underset{\sim}{T}_{ijs}$ осуществляется поглощение компонентом $0/x^{min}_{ijs}$ и $0/x^{max}_{ijs}$ соответст-

венно ряда других компонентов согласно выражений $x_{ijs}^{min} = \bigvee_{\substack{q=1 \\ при\ U1}}^{M-1} x_{ijsq}$ и $x_{ijs}^{max} = \bigwedge_{\substack{q=M \\ при\ U2}}^{r} x_{ijsq}$, где $U_1 \stackrel{def}{=} \forall x_{ijsq} < x_{ijsM} : \mu_{ijsq} = 0$, $U_2 \stackrel{def}{=} \forall x_{ijsq} > x_{ijsM} : \mu_{ijsq} = 0,$ а x_{ijsM} и M – соответственно мода $\underset{\sim}{T}_{ijs}$ и ее порядковый номер.

Далее, с учетом этих преобразований и выражения (9), определим набор промежуточных термов в виде

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

$$\mu_{ijsr-\gamma+1} / x_{ijsr-\gamma+1}\} = \{\mu_{ijs\beta} / x_{ijs\beta},\ \mu_{ijs\beta+1} / x_{ijs\beta+1},\ ...,$$

$$\mu_{ijsr-\gamma} / x_{ijsr-\gamma}, \mu_{ijsr-\gamma+1} / x_{ijsr-\gamma+1}\}, \qquad (13)$$

где $\mu_{ijs\beta} / x_{ijs\beta} = 0 / x_{ijs\beta} = 0/x_{ijs}^{min}$ и $\mu_{ijsr-\gamma+1} / x_{ijsr-\gamma+1} = 0 / x_{ijsr-\gamma+1} = 0/x_{ijs}^{max}$, а β и γ – количество поглощенных $0 / x_{ijsq}$ соответственно слева и справа от $x_{ijs(M)}$. Таким образом, формируются подмножества эталонов

$$\underset{\sim}{T}^{e}_{ijs} = \{\bigcup_{q=1}^{r_s} \mu^{e}_{ijsq} / x^{e}_{ijsq}\} = \{\mu^{e}_{ijs1} / x^{e}_{ijs1},\ \mu^{e}_{ijs2} / x^{e}_{ijs2}, ...,$$

$$\mu^{e}_{ijsr_s-1} / x^{e}_{ijsr_s-1}, \mu^{e}_{ijsr_s} / x^{e}_{ijsr_s}\}\ \ (q = \overline{1, r_s}), \qquad (14)$$

где $\mu^{e}_{ijs1} / x^{e}_{ijs1} = \mu_{ijs\beta} / x_{ijs\beta}$, $\mu^{e}_{ijs2} / x^{e}_{ijs2} = \mu_{ijs\beta+1} / x_{ijs\beta+1}$, …, $\mu^{e}_{ijsr_s-1} / x^{e}_{ijsr_s-1} = \mu_{ijsr-\gamma} / x_{ijsr-\gamma}$, $\mu^{e}_{ijsr_s} / x^{e}_{ijsr_s} = \mu_{ijsr-\gamma+1} / x_{ijsr-\gamma+1}$.

Шаг 3. Если при реализации второго шага для выражения (13) $\exists\, \underset{\sim}{T}'_{ijs} : \{0/x_{ijs}^{min}\} \in \varnothing$ или $\exists\, \underset{\sim}{T}'_{ijs} : \{0/x_{ijs}^{max}\} \in \varnothing$ (т.е. $\mu_{ijs\beta} \neq 0$, $\mu_{ijsr-\gamma+1} \neq 0$), то для таких термов дальнейшее формирование подмножества $\underset{\sim}{T}^{e}_{ijs}$ осуществляется путем расширения $\underset{\sim}{T}'_{ijs}$ посредством введения дополнительных компонент $\mu_{ijs\beta-1} / x_{ijs\beta-1}$ и $\mu_{ijsr-\gamma+2} / x_{ijsr-\gamma+2}$.

С учетом этого, наборы промежуточных термов будут иметь следующий вид $\underset{\sim}{T}'_{ijs} =$

$$\{\mu_{ijs\beta-1} / x_{ijs\beta-1}, \mu_{ijs\beta} / x_{ijs\beta}, ..., \bigcup_{q=\beta+1}^{r-\gamma} \mu_{ijsq} / x_{ijsq}, ...,$$

$$\mu_{ijsr-\gamma+1} / x_{ijsr-\gamma+1}, \mu_{ijsr-\gamma+2} / x_{ijsr-\gamma+2}\} = \{\mu_{ijs\beta-1} / x_{ijs\beta-1},$$

$$\mu_{ijs\beta} / x_{ijs\beta}, ..., \mu_{ijsr-\gamma+1} / x_{ijsr-\gamma+1}, \mu_{ijsr-\gamma+2} / x_{ijsr-\gamma+2}\},$$

где $x_{ijs\beta-1} = x_{ijs\beta}$, $x_{ijsr-\gamma+2} = x_{ijsr-\gamma+1}$, а $\mu_{ijs\beta-1} = \mu_{ijsr-\gamma+2} = 0$.

Таким образом, компоненты подмножества эталонов $\underset{\sim}{T}^{e}_{ijs}$ в выражении (14) будут определятся как $\mu^{e}_{ijs1} / x^{e}_{ijs1} = \mu_{ijs\beta-1} / x_{ijs\beta-1}, \mu^{e}_{ijs2} / x^{e}_{ijs2} = \mu_{ijs\beta} / x_{ijs\beta}, ..., \mu^{e}_{ijsr_s-1} / x^{e}_{ijsr_s-1} = \mu_{ijsr-\gamma+1} / x_{ijsr-\gamma+1}$, $\mu^{e}_{ijsr_s} / x^{e}_{ijsr_s} = \mu_{ijsr-\gamma+2} / x_{ijsr-\gamma+2}$.

Например, по выражению (12) при $i = 2$, $j = 3$, $r = 5$ сформируем $\mathbf{T^e_{23}} \in \mathbf{T^e}$ т.е.

$$\mathbf{T^e_{23}} = \bigcup_{s=1}^{5} \underset{\sim}{T}^{e}_{23s} = \{\underset{\sim}{T}^{e}_{231},\ \underset{\sim}{T}^{e}_{232},\ \underset{\sim}{T}^{e}_{233},\ \underset{\sim}{T}^{e}_{234},\ \underset{\sim}{T}^{e}_{235}\} =$$

$$\{\underset{\sim}{T}^{e}_{DSKOП1},\ \underset{\sim}{T}^{e}_{DSKOП2},\ \underset{\sim}{T}^{e}_{DSKOП3},\ \underset{\sim}{T}^{e}_{DSKOП4},\ \underset{\sim}{T}^{e}_{DSKOП5}\} = \{\underset{\sim}{OM}^{e}_{23},\ \underset{\sim}{M}^{e}_{23},\ \underset{\sim}{C}^{e}_{23},\ \underset{\sim}{Б}^{e}_{23},\ \underset{\sim}{OБ}^{e}_{23}\}$$

$(s = \overline{1,5})$, где члены подмножества $\mathbf{T^e_{23}}$ – $\underset{\sim}{OM}^{e}_{23}$, $\underset{\sim}{M}^{e}_{23}$, $\underset{\sim}{C}^{e}_{23}$, $\underset{\sim}{Б}^{e}_{23}$, $\underset{\sim}{OБ}^{e}_{23}$ являются эталонными НЧ.

Шаг 1. Преобразуем нечеткие термы $\underset{\sim}{OM}_{23}$, $\underset{\sim}{M}_{23}$, $\underset{\sim}{C}_{23}$, $\underset{\sim}{Б}_{23}$ и $\underset{\sim}{OБ}_{23}$ таким образом, чтобы для всех $\underset{\sim}{T}_{23s}$ было справедливо отношение порядка, т.е. $\forall x_{23sq} : x_{23sq} < x_{23sq+1}$ $(q = \overline{1,4})$. Если в качестве компонентов таких термов использовать конкретные значения полученные в примере этапа 4, то для них такое отношение будет истинным. Так, например, для $\underset{\sim}{OM}_{23}$ это $x_{2311} < x_{2312} < x_{2313} < x_{2314} < x_{2315} = 0{,}008 < 0{,}063 < 0{,}25 < 0{,}5 < 1$.

Шаг 2. Для $\underset{\sim}{OM}_{23}$ (где мода $x_{231M} = x_{2311} = 0{,}008$, а ее порядковый номер $M = 1$) при условии U_2 (т.е. $\mu_{2313} = \mu_{2314} = \mu_{2315} = 0$) осуществляется поглощение одним компонентом $0/x_{231}^{max}$ ряда других согласно выражения $x_{231}^{max} = x_{2313} \wedge x_{2314} \wedge x_{2315} = 0{,}25 \wedge 0{,}5 \wedge 1 = 0{,}25$ $(q = \overline{1,5})$. Таким образом $\mu_{2313} / x_{2313} = 0/0{,}25$, $\mu_{2314} / x_{2314} = 0 / 0{,}5$ и $\mu_{2315} / x_{2315} = 0 / 1$ поглощаются компонентом $\mu_{2313} / x_{2313} = 0/0{,}25$.

Аналогичным образом для $\underset{\sim}{M}_{23}$ (где $x_{232M} = x_{2322} = 0{,}063$, а $M = 2$) при условии U_2 (т.е. $\mu_{2324} = \mu_{2325} = 0$) компонент $0/x_{232}^{max} = \mu_{2324} / x_{2324} = 0 / 0{,}5$ согласно выражения $x_{232}^{max} = x_{2324} \wedge x_{2325} = 0{,}5 \wedge 1 = 0{,}5$ $(q = \overline{2,5})$ поглощает компоненты $\mu_{2324} / x_{2324} = 0 / 0{,}5$ и $\mu_{2325} / x_{2325} = 0/1$.

Далее видно, что для НЧ $\underset{\sim}{C}_{23}$ условие U_1 и U_2 не выполняется и поэтому операция поглощения не осуществляется.

Для $\underset{\sim}{Б}_{23}$ (где $x_{234M} = x_{2344} = 0{,}5,\ M = 4$) при условии U_1 ($\mu_{2341} = \mu_{2342} = 0$) компонент $0/x_{234}^{min}$ $= \mu_{2342} / x_{2342} = 0/0{,}063$ согласно выражения $x_{234}^{\min} = x_{2341} \vee x_{2342} = 0{,}008 \vee 0{,}063 = 0{,}063$ $(q = \overline{1,3})$ поглощает компоненты $\mu_{2341} / x_{2341} = 0/0{,}008$ и $\mu_{2342} / x_{2342} = 0/0{,}063$.

Аналогично для $\underset{\sim}{ОБ}_{23}$ ($x_{235M} = x_{2355} = 1$, $M = 5$) при условии U_1 ($\mu_{2351} = \mu_{2352} = \mu_{2353} = 0$) компонент $0/x_{235}^{\min} = \mu_{2353} / x_{2353} = 0/0{,}25$ согласно выражения $x_{235}^{\min} = x_{2351} \vee x_{2352} \vee x_{2353} = 0{,}008 \vee 0{,}063 \vee 0{,}25 = 0{,}25$ $(q = \overline{1,4})$ поглощает компоненты $\mu_{2351} / x_{2351} = 0{,}008$, $\mu_{2352} / x_{2352} = 0/0{,}063$ и $\mu_{2353} / x_{2353} = 0/0{,}25$.

Далее, с учетом этих преобразований и выражения (13) определим набор промежуточных термов в виде $\underset{\sim}{T}'_{231} = \underset{\sim}{T}'_{DSKOП1} = \underset{\sim}{OM}'_{23} =$ $\{\mu_{2311} / x_{2311}, \mu_{2312} / x_{2312}, \mu_{2313} / x_{2313}\} = \{1/0{,}008;$ $0{,}3/0{,}063;\ 0/0{,}25\}$, $\underset{\sim}{T}'_{232} = \underset{\sim}{T}'_{DSKOП2} = \underset{\sim}{M}'_{23} = \{\mu_{2321} / x_{2321},$ $\mu_{2322} / x_{2322}, \mu_{2323} / x_{2323}, \mu_{2324} / x_{2324}\} = \{0{,}55/0{,}008;$ $1/0{,}063;\ 0{,}24/0{,}25;\ 0/0{,}5\}$, $\underset{\sim}{T}'_{233} = \underset{\sim}{T}'_{DSKOП3} = \underset{\sim}{C}'_{23} =$ $\{\mu_{2331} / x_{2331}, \mu_{2332} / x_{2332}, \mu_{2333} / x_{2333}, \mu_{2334} / x_{2334},$ $\mu_{2335} / x_{2335}\} = \{0/0{,}008;\ 0{,}35/0{,}063;\ 1/0{,}25;\ 0{,}32\ /0{,}5;$ $0/1\}$, $\underset{\sim}{T}'_{234} = \underset{\sim}{T}'_{DSKOП4} = \underset{\sim}{Б}'_{23} = \{\mu_{2342} / x_{2342},$ $\mu_{2343} / x_{2343}, \mu_{2344} / x_{2344}, \mu_{2345} / x_{2345}\} = \{0/0{,}063;$ $0{,}8/0{,}25;\ 1/0{,}5;\ 0{,}9/1\}$, $T'_{235} = \underset{\sim}{T}'_{DSKOП5} = \underset{\sim}{ОБ}'_{23} =$ $\{\mu_{2353} / x_{2353}, \mu_{2354} / x_{2354}, \mu_{2355} / x_{2355}\} = \{0/0{,}25;$ $0{,}68/0{,}5;\ 1/1\}$.

Поскольку $\mu_{2331} / x_{2331} = 0/x_{233}^{min} = 0 / x_{2331}$ и $\mu_{2335} / x_{2335} = 0/x_{233}^{max} = 0/x_{2335}$, то после шага 2 для $\underset{\sim}{C}'_{23}$ согласно выражения (14) формируются эталонные значения, т.е. $\underset{\sim}{T}^e_{233} = \underset{\sim}{T}^e_{DSKOП3} = \underset{\sim}{C}^e_{23} =$ $\{\mu^e_{2331} / x^e_{2331}, \mu^e_{2332} / x^e_{2332}, \mu^e_{2333} / x^e_{2333}, \mu^e_{2334} / x^e_{2334},$ $\mu^e_{2335} / x^e_{2335}\} = \{0/0{,}008;\ 0{,}35/0{,}063;\ 1/0{,}25;\ 0{,}32\ /0{,}5;$ $0/1\}$, где $\mu^e_{2331} / x^e_{2331} = \mu_{2331} / x_{2331}$, $\mu^e_{2332} / x^e_{2332} =$ μ_{2332} / x_{2332}, $\mu^e_{2333} / x^e_{2333} = \mu_{2333} / x_{2333}$, $\mu^e_{2334} / x^e_{2334} =$ μ_{2334} / x_{2334} и $\mu^e_{2335} / x^e_{2335} = \mu_{2335} / x_{2335}$.

Шаг 3. При реализации второго шага в выражении (13) для набора промежуточных термов $\underset{\sim}{OM}'_{23}$ и $\underset{\sim}{M}'_{23}$ $\exists\, \underset{\sim}{T}'_{231} : \{0/x_{231}^{min}\} \in \varnothing$ и $\exists\, \underset{\sim}{T}'_{232}$: $\{0/x_{232}^{min}\} \in \varnothing$ (т.е. $\mu_{2311} = 1 \neq 0$ и $\mu_{2321} = 1 \neq 0$), а для $\underset{\sim}{Б}'_{23}$ и $\underset{\sim}{ОБ}'_{23}$ $\exists\, \underset{\sim}{T}'_{234} : \{0/x_{234}^{max}\} \in \varnothing$ и $\exists\, \underset{\sim}{T}'_{235}$: $\{0/x_{235}^{max}\} \in \varnothing$ (т.е. $\mu_{2345} = 0{,}93 \neq 0$ и $\mu_{2355} = 1 \neq 0$), то формирование подмножеств $\underset{\sim}{T}^e_{231}$, $\underset{\sim}{T}^e_{232}$ и $\underset{\sim}{T}^e_{234}$, $\underset{\sim}{T}^e_{235}$ осуществим за счет расширения $\underset{\sim}{T}'_{231}$, $\underset{\sim}{T}'_{232}$ и $\underset{\sim}{T}'_{234}$, $\underset{\sim}{T}'_{235}$ (см. (13)) посредством введения дополнительных компонент $\mu_{231\beta-1} / x_{231\beta-1} =$ $0/0{,}008$, $\mu_{232\beta-1} / x_{232\beta-1} = 0/0{,}008$ и $\mu_{234\text{г}-\gamma+2} / x_{234\text{г}-\gamma+2} =$ $0/1$, $\mu_{235\text{г}-\gamma+2} / x_{235\text{г}-\gamma+2} = 0/1$ соответственно.

С учетом этого, набор промежуточных термов для $\underset{\sim}{OM}'_{23}$ будет иметь следующий вид $\underset{\sim}{T}'_{231} = \underset{\sim}{T}'_{DSKOП1} = \underset{\sim}{OM}'_{23} = \{\mu_{2311} / x_{2311}, \mu_{2312} / x_{2312},$ $\mu_{2313} / x_{2313}\} = \{0/0{,}008;\ 1/0{,}008;\ 0{,}3/0{,}063;\ 0/0{,}25\}$, где $\mu_{231\beta-1} = 0$. Аналогичным способом получаем промежуточные термы для $\underset{\sim}{M}'_{23}$, $\underset{\sim}{Б}'_{23}$ и $\underset{\sim}{ОБ}'_{23}$, где $\mu_{232\beta-1} = \mu_{234\text{г}-\gamma+2} = \mu_{235\text{г}-\gamma+2} = 0$.

Таким образом, компоненты подмножества эталонов $\underset{\sim}{T}^e_{231}$ согласно выражения (14) будут определятся как $\mu^e_{2311} / x^e_{2311} = 0/0{,}008$, $\mu^e_{2312} / x^e_{2312} =$ $1/0{,}008$, $\mu^e_{2313} / x^e_{2313} = 0{,}3/0{,}063$, $\mu^e_{2314} / x^e_{2314} = 0/0{,}25$ и аналогичным образом для $\underset{\sim}{T}^e_{232}$, $\underset{\sim}{T}^e_{234}$, $\underset{\sim}{T}^e_{235}$.

Далее согласно выражения (14) для $\underset{\sim}{OM}'_{23}$, $\underset{\sim}{M}'_{23}$, $\underset{\sim}{Б}'_{23}$ и $\underset{\sim}{ОБ}'_{23}$ можем сформировать эталонные значения, т.е. $\underset{\sim}{T}^e_{231} = \underset{\sim}{T}^e_{DSKOП1} = \underset{\sim}{OM}^e_{23} =$ $\{\mu^e_{2311} / x^e_{2311}, \mu^e_{2312} / x^e_{2312}, \mu^e_{2313} / x^e_{2313}\} = \{0/0{,}008;$ $1/0{,}008;\ 0{,}3/0{,}063;\ 0/0{,}25\}$, $\underset{\sim}{T}^e_{232} = \underset{\sim}{T}^e_{DSKOП2} = \underset{\sim}{M}^e_{23} =$ $\{\mu^e_{2321} / x^e_{2321}, \mu^e_{2322} / x^e_{2322}, \mu^e_{2323} / x^e_{2323}, \mu^e_{2324} / x^e_{2324}\} =$ $\{0/0{,}008;\ 0{,}55/0{,}008;\ 1/0{,}063;\ 0{,}24/0{,}25;\ 0/0{,}5\}$, $\underset{\sim}{T}^e_{234} = \underset{\sim}{T}^e_{DSKOП4} = \underset{\sim}{Б}^e_{23} = \{\mu^e_{2342} / x^e_{2342}, \mu^e_{2343} / x^e_{2343},$ $\mu^e_{2344} / x^e_{2344}, \mu^e_{2345} / x^e_{2345}\} = \{0/0{,}063;\ 0{,}8/0{,}25;\ 1/0{,}5;$ $0{,}9/1;\ 0/1\}$, $\underset{\sim}{T}^e_{235} = \underset{\sim}{T}^e_{DSKOП5} = \underset{\sim}{ОБ}^e_{23} = \{\mu^e_{2353} / x^e_{2353},$ $\mu^e_{2354} / x^e_{2354}, \mu^e_{2355} / x^e_{2355}\} = \{0/0{,}25;\ 0{,}68/0{,}5;\ 1/1;\ 0/1\}$.

Этап 6 – визуализация лингвистических эталонов. Реализация этого этапа основывается на построении геометрического образа всех эталонных НЧ (14) принадлежащих согласно выражения (12) подмножеству $\mathbf{T}^{\mathbf{e}}_{\mathbf{ij}}$. Геометрическое место точек на плоскости определяется посредством ломаной соединяющей точки, отображающие компоненты НЧ $\underset{\sim}{T}^{e}_{ijs}$ в порядке возрастания их суппортов. Визуализация одного типового эталонного терма (14) представлена в виде ломанной ⟶ на рис. 1.

Например, для визуализации подмножества эталонов $\mathbf{T}^{\mathbf{e}}_{\mathbf{23}} = \mathbf{T}^{\mathbf{e}}_{\mathbf{DSKOП}}$ воспользуемся сформированным по выражению (12) и (14) эталонными НЧ (см. пример этапа 5): $\underset{\sim}{OM}^{e}_{23} = \{0/0{,}008;\ 1/0{,}008;\ 0{,}3/0{,}063;\ 0/0{,}25\}$, $\underset{\sim}{M}^{e}_{23} = \{0/0{,}008;\ 0{,}55/0{,}008;\ 1/0{,}063;\ 0{,}24/0{,}25;\ 0/0{,}5\}$, $\underset{\sim}{C}^{e}_{23} = \{0/0{,}008;\ 0{,}35/0{,}063;\ 1/0{,}25;\ 0{,}32\ /0{,}5;\ 0/1\}$, $\underset{\sim}{Б}^{e}_{23} = \{0/0{,}063;\ 0{,}8/0{,}25;\ 1/0{,}5;\ 0{,}9/1;\ 0/1\}$, $\underset{\sim}{OБ}^{e}_{23} = \{0/0{,}25;\ 0{,}68/0{,}5;\ 1/1;\ 0/1\}$. На их основе посредством соединения точек, отображаемых соответствующими компонентами эталонных НЧ $\underset{\sim}{OM}^{e}_{23}$, $\underset{\sim}{M}^{e}_{23}$, $\underset{\sim}{C}^{e}_{23}$, $\underset{\sim}{Б}^{e}_{23}$, $\underset{\sim}{OБ}^{e}_{23}$ строится пять ломанных ⟶, ⟶, ⟶, ⟶, ⟶, которые графически интерпретируются на рис. 2.

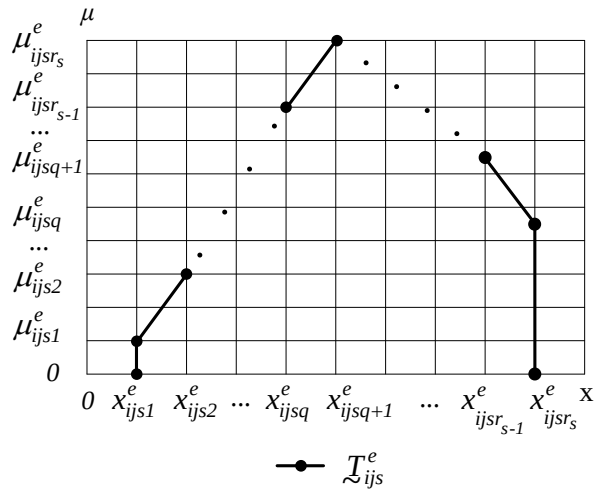

Рис. 1. Лингвистический эталон НЧ $\underset{\sim}{T}^{e}_{ijs}$

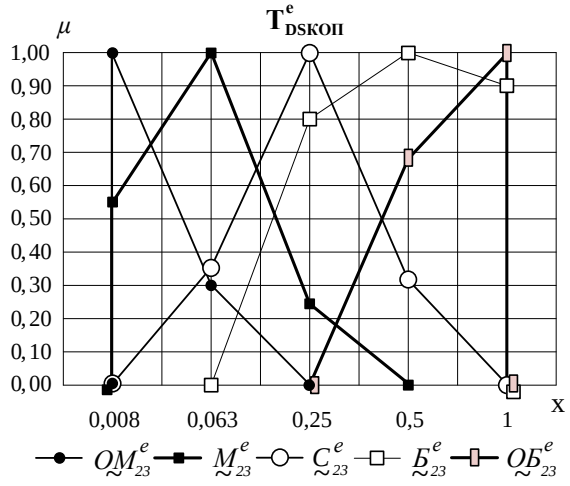

Рис. 2. Лингвистические эталоны подмножества $\mathbf{T}^{\mathbf{e}}_{\mathbf{DSKOП}}$

Предложенный в работе МФЛЭ для систем выявления вторжений, за счет использования множеств идентификаторов лингвистических оценок и идентификаторов интервалов, базовой и производной матрицы частот, дает возможность отображать суждения эксперта для характеристики текущего состояния параметров относительно кибератаки, формировать на заданных интервалах частоты встречаемости экспертных оценок и построения подмножеств нечетких термов, что позволяет формализовать процесс получения эталонных значений параметров заданных групп лингвистических переменных, характеризующих конкретную среду окружения.

ЛИТЕРАТУРА

[1]. Корченко А.А. Система выявления аномального состояния в компьютерных сетях / А.А. Корченко // Безпека інформації. – 2012. – № 2 (18). – С. 80-84.

[2]. Корченко А.А. Система формирования нечетких эталонов сетевых параметров / А.А. Корченко // Захист інформації. – 2013. – Т.15, №3. – С. 240-246.

[3]. Корченко А.А. Система формирования эвристических правил для оценивания сетевой активности / А.А. Корченко // Захист інформації. – 2013. – №4. Т.15. – С. 353-359.

[4]. Стасюк А.И. Метод выявления аномалий порожденных кибератаками в компьютерных сетях / А.И. Стасюк, А.А. Корченко // Захист інформації. – 2012. – №4 (57). – С. 129-134.

[5]. Корченко А.Г. Построение систем защиты информации на нечетких множествах [Текст] : Теория и практические решения / А.Г. Корченко. – К. : МК-Пресс, 2006. – 320 с.

[6]. Стасюк А.И. Базовая модель параметров для построения систем выявления атак / А.И. Стасюк, А.А. Корченко // Захист інформації. – 2012. – № 2 (55). – С. 47-51.

REFERENCES

[1]. Korchenko A.A. Anomaly-based detection system in computer networks, Bezpeka informacii, 2012, №2 (18), pp. 80-84.

[2]. Korchenko A.A. The system development of fuzzy standards of network parameters, Zahist ìnformacìï, T.15, №3, 2013, pp. 240-246.
[3]. Korchenko A.A. The system of heuristic rules formation for network activity assessment, Zahist ìnformacìï, T.15, №4, 2013, pp. 353-359.
[4]. 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.
[5]. Korchenko A.G. The development of information protection systems based on the fuzzy sets, The theory and practical solutions, Kuev, 2006, 320 p.
[6]. Stasiuk A.I., Korchenko A.A. The basic model of parameters in attack detection (Identification) systems construction, Zahist ìnformacìï, 2012, №2 (55), pp. 47-51.

МЕТОД ФОРМУВАННЯ ЛІНГВІСТИЧНИХ ЕТАЛОНІВ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Одним із рішень забезпечення інформаційної безпеки є системи виявлення вторгнень, засновані на аномальному принципі. Для побудови такого роду систем використовується метод виявлення аномалій, породжених кібератаками в інформаційних системах. У цьому методі процес формування різних еталонів досить трудомісткий і практично не формалізований, що знижує ефективність його використання. З метою компенсації цього недоліку пропонується метод, який базується на математичних моделях і методах нечіткої логіки та реалізується за допомогою шести базових етапів: формування підмножин ідентифікаторів лінгвістичних оцінок, формування базової матриці частот, формування похідної матриці частот, формування нечітких термів, формування еталонних нечітких чисел, візуалізація лінгвістичних еталонів. Метод дозволяє удосконалити процес формалізації отримання лінгвістичних еталонів параметрів для підвищення ефективності побудови відповідних систем виявлення вторгнень.

Ключові слова: кібератаки, аномалії, нечіткі еталони, метод формування лінгвістичних еталонів, системи виявлення вторгнень, системи виявлення аномалій, системи виявлення атак, виявлення аномалій в комп'ютерних мережах.

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

One of the information security solutions are the intrusion detection systems based on the principle of anomaly. To develop such a kind of systems the anomaly detection method generated by cyberattacks in information systems is used. In this method, the process of formation of various standards is quite complicated and practically is not formalized, that reduces the efficiency of its use. In order to compensate for this drawback it is proposed the method which is based on mathematical models and methods of fuzzy logic and is implemented through the six basic stages: formation of subsets of linguistic assessments identifiers, formation of the basic matrix of frequencies, formation of a derivative matrix of frequencies, the formation of fuzzy terms, formation of fuzzy numbers, the visualization of linguistic standards. The method enables to improve the process of formalization of linguistic standards to increase the efficiency of the corresponding detection intrusion systems.

Keywords: cyber attacks, anomalies, fuzzy standards, the formation method of linguistic standards, intrusion detection systems, anomaly detection systems, attack detection systems, anomaly detection in computer networks.

Корченко Анна Олександрівна, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: annakor@ukr.net
Корченко Анна Александровна, кандидат технических наук, доцент кафедры безопасности информационных технологий Национального авиационного университета.
Korchenko Anna, PhD in Eng., Associate Professor of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

УДК 511.512

ПРОГРАММНО-МОДЕЛИРУЮЩИЙ КОМПЛЕКС КРИПТОГРАФИЧЕСКИХ AES-ПОДОБНЫХ ПРИМИТИВОВ НЕЛИНЕЙНОЙ ПОДСТАНОВКИ

Александр Белецкий, Анатолий Белецкий, Денис Навроцкий, Александр Семенюк

Любой итеративный блочный шифр должен содержать хотя бы один нелинейный примитив. Отсутствие нелинейных преобразований существенно снижает криптостойкость шифра, так как, сколько бы не было в раундах различных линейных примитивов, их совокупность может быть сведена к одному эквивалентному, что, как следствие, приводит к угрозе достаточно легкого взлома шифра. В работе изложена методика синтеза примитивов нелинейной