A CONCEPTUAL MODEL OF THE MICROWAVE CHANNEL OF INFORMATION LEAKAGE BY THE POWER SUPPLY CIRCUIT

For the construction of the microwave filter devices to prevent information leakage on the supply lines should take into account the impact of external screens. Existing methods for the synthesis filtering devices are based on the mathematical model the two-wire transmission line, excluding the effect of shielding the outer envelope. As a result, the frequency response function of the filter is different from the experimental, which leads to deterioration in the band rejection filter. Proposed as a conceptual mathematical model of the filter element model coupled transmission line. The conceptual model takes into account the effect of shielding the outer shell and increases the accuracy of calculating the filtration devices in the power supply circuit.

Index Terms: coupled transmission line, eight-pole network, four-pole network, even and odd excitation, wave impedance.

Козловский Валерий Валерьевич, кандидат технических наук, доцент Государственного университета информационно-коммуникационных технологий.
E-mail: valerey@ukr.net

Козловський Валерій Валерійович, кандидат технічних наук, доцент Державного університету інформаційно-комунікаційних технологій.
Kozlowskiy Valeriy, Ph.D. in Eng., associate professor of the State University of Information and Communication Technologies.

Лысенко Роман Михайлович, аспирант Института специальной связи и защиты информации Национального технического университета Украины «КПИ», главный научный сотрудник Государственной службы специальной связи и защиты информации Украины.
E-mail: romanukr@list.ru

Лисенко Роман Михайлович, аспірант Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «КПІ», головний науковий співробітник Державної служби спеціального зв'язку та захисту інформації України.
Lysenko Roman, PhD student of Institute of Special Communication and Information Security of National Technical University of Ukraine «KPI», Chief Scientific Officer of the State Service of Special Communication and Information Protection of Ukraine.

УДК 004.056.53(045)

СИСТЕМА ФОРМИРОВАНИЯ НЕЧЕТКИХ ЭТАЛОНОВ СЕТЕВЫХ ПАРАМЕТРОВ

Анна Корченко

На основе известного метода выявления аномалий порожденных кибератаками разработана соответствующая система, для поддержки функционирования которой необходима реализация средства формирования нечетких эталонов, ориентированного на измерение текущих значений параметров сетевого трафика с целью выявления подозрительной активности в среде окружения. Для решения такой задачи предложено новое структурное решение соответствующей системы, состоящей из регистра эталонов, атак и параметров, а также блоков коммутации параметров, связывания атаки с параметром, формирования совокупности термов, формирования эталонов, регистра эталонов и процессора визуализации эталонов. Эта разработка может быть реализована программно или программно-аппаратно и ориентирована на измерение текущих значений параметров сетевого трафика с целью идентификации аномального состояния.

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

Использование методов и моделей нечетких множеств для построения средств обнаружения аномалий, порожденных атакующими действиями, позволит усовершенствовать существующие системы выявления вторжений и, путем контроля активности в среде окружения, идентифицировать опасные аномальные состояния. Для этого в работах [1-2] разработана базовая модель параметров и универсальная модель эталонов лингвистических переменных (ЛП), которые за счет сформированных множеств пар, связывающих тип атаки с параметрами и набором логико-лингвистических связок, позволяют формализовать процесс построения эталонных значений для заданной среды окружения, отображать и устанавливать соответствие между типом атаки и необходимыми для ее идентификации атрибутами, а также измерять аномальное

состояние сетевой активности, характерное для определенного множества кибератак в компьютерных системах. В работе [3] построена модель эвристических правил, которая за счет предложенного множества эталонных параметров, матриц инициализации для логико-лингвистических связок и лингвистических идентификаторов, позволяет формализовать процесс формирования множеств соответствующих правил для выявления аномального состояния, порожденного определенным типом атак в компьютерных сетях. Для идентификации аномалий в работе [4] разработан метод выявления аномалий порожденных кибератаками в компьютерных сетях, реализация которого осуществляется за восемь базовых этапов: выбор метода обработки нечетких данных; выбор метода определения коэффициента важности; формирование множеств атак и параметров; формирование эталонов параметров; фаззификация параметров; формирование множества эвристических правил; определение матриц инициализации; формирование результата. В основу этого метода положены разработанная [1-3, 5] базовая модель параметров, универсальная модель эталонов и модель эвристических правил, которые в комплексе с текущими параметрами сформированными в нечетко определенной слабоформализованной среде, позволяют строить средства обнаружения несигнатурных и новых типов кибератак, направленных на ресурсы информационных систем. Также в работе [6] предложено структурное решения системы выявления аномального состояния в компьютерных сетях, состоящее из: подсистемы первичной обработки; подсистемы формирования нечетких эталонов (НЭ); подсистемы формирования эвристических правил; модулей нечеткой арифметики, логического вывода и визуализации. Это решение используется для совершенствования систем сетевой безопасности, которое основывается на реализации указанного метода обнаружения аномалий [4] и ориентировано на осуществление контроля активности в определенной среде окружения.

Для поддержки функционирования такой системы актуальным является разработка соответствующего средства обеспечивающего эффективную работу указанной подсистемы формирования НЭ сетевых параметров. В связи с этим, целью данной работы является создание алгоритмического обеспечения и нового структурного решения, которые могут использоваться на практике для расширения функциональных возможностей современных систем обнаружения вторжений.

Для достижения поставленной цели воспользуемся методом выявления аномалий порожденных кибератаками в компьютерных сетях [4]. На его основе предлагается новое структурное решение соответствующей системы формирования НЭ сетевых параметров (рис. 1), ориентированной на измерение текущих значений параметров сетевого трафика с целью идентификации аномального состояния.

Система содержит:

– регистр атак и параметров (РАП), предназначенный для приема и хранения текущих значений идентификатора типа атаки AT_i $(i = \overline{1,n})$ и параметров P_i $(i = \overline{1,m})$ [1, 6];

– блок коммутации параметров (БКП), осуществляющий формирование потоков параметров соответствующих типу атаки;

– блок связывания атаки с параметром (БСАП) [6], ориентированный на реализацию связи идентификатора типа атаки и соответствующих ей параметров;

– блок формирования совокупности термов (БФСТ), применяемый для генерирования заданного множества T_{ij}^{ef} [1];

– блок формирования эталонов (БФЭ), осуществляющий вычисление для каждого T_{ij}^{ef} соответствующего эталонного нечеткого числа (НЧ) [2];

– регистр эталонов (РЭ), служащий для приема и временного хранения вычисленных эталонных НЧ;

– процессор визуализации эталонов (ПВЭ), предназначенный для отображения в графическом виде полученных эталонных НЧ.

Согласно разработанному алгоритму (рис. 2) система (рис. 1) функционирует следующим образом. В регистр атак (РА) и параметров (РП), обозначаемый РАП, предварительно заносятся и хранятся на протяжении всего процесса вычислений соответственно текущие значения идентификаторов AT_i, $i = \overline{1,n}$ и входных параметров P_j, $j = \overline{1,m}$ (см. соответственно вершины 1, 2 и 3, 4 на рис. 2).

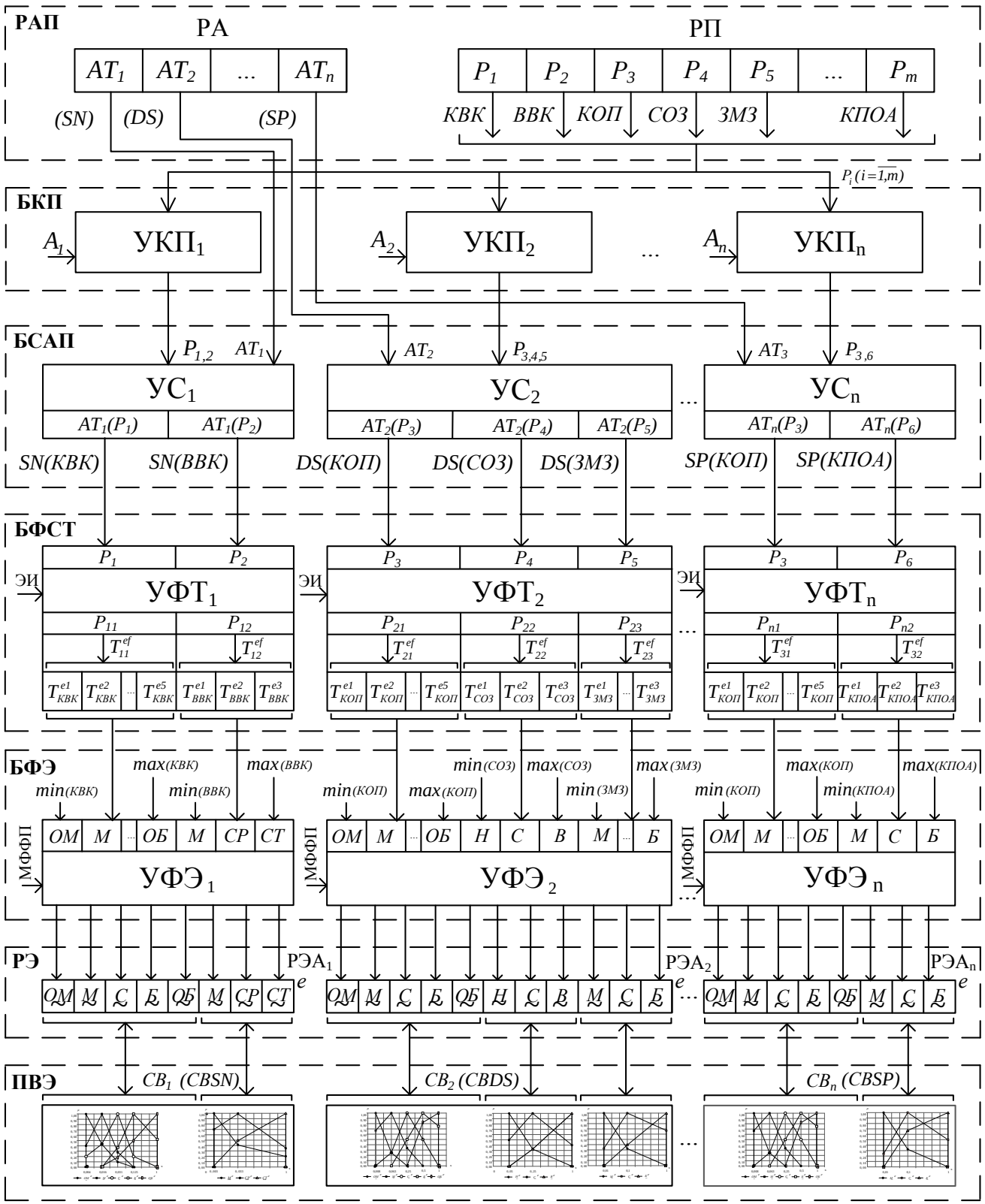

Рис. 1. Структура системы формирования НЭ сетевых параметров

Далее, в соответствующих узлах формирования термов (УФТ$_i$, $i=\overline{1,n}$) БФСТ генерируется значения T_{ij}^{ef} ($f=\overline{1,r}$; $i=\overline{1,n}$; $j=\overline{1,m}$) для всех P_i ($i=\overline{1,m}$).

Количество таких термов и их лингвистическая интерпретация определяется по экспертной информации, полученной на основе суждений специалистов соответствующей предметной области [7, 8].

Для каждого УФТ$_i$ БФСТ относительно экспертной информации определяются в каждом цикле свои значения j' и f' (см. вершины 7-10 на рис. 2), согласно которых формируются тре-

буемые наборы T_{ij}^{ef} для всех P_i. Например, при $m= j' =2$, $f' =5$ и при $i=3$, $j' =2$, $f' =3$ на выходе УФТ$_1$ формируется массив (вектор):

$$\text{УФТ}_1(\{T_{11}^{e1}, T_{11}^{e2}, T_{11}^{e3}, T_{11}^{e4}, T_{11}^{e5}\},\{T_{12}^{e1}, T_{12}^{e2}, T_{12}^{e3}\})=$$

$$\text{УФТ}_1(\{T_{КВК}^{e1}, T_{КВК}^{e2}, T_{КВК}^{e3}, T_{КВК}^{e4}, T_{КВК}^{e5}\},\{T_{ВВК}^{e1}, T_{ВВК}^{e2}, T_{ВВК}^{e3}\}).$$

После получения требуемого набора термов для каждой AT_i в узлах формирования эталонов (УФЭ$_i$) БФЭ определяются конкретные значения НЧ по каждому T_{ij}^{ef}. При реализации этой процедуры необходимо задать граничные значения для всех P_i ($i=\overline{1,m}$), т.е. $\min p_i$ и $\max p_i$ (см. вершины 11 и 12 на рис. 2) (например, для P_1 и P_2 границы $\min p_1 = \min(КВК)$, $\max(p_1) = \max(КВК)$ и $\min p_2 = \min(ВВК)$, $\max(p_2) = \max(ВВК)$), а также согласно установленных критериев [7], выбрать метод формирования функций принадлежности (см. этап 2 в [4]).

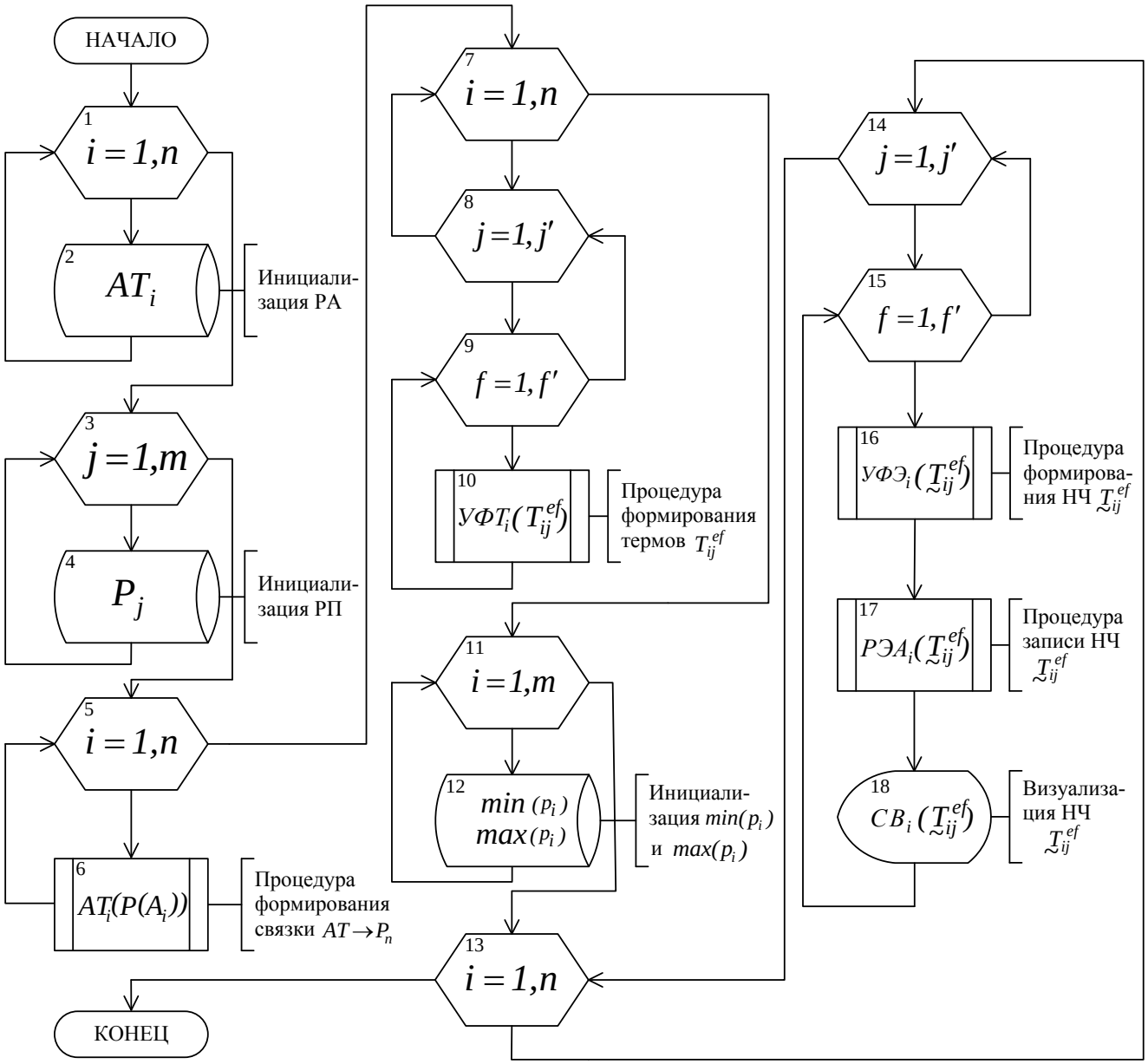

Рис. 2. Алгоритм работы системы формирования НЭ сетевых параметров

Например, эти термы могут быть соответственно отображены на универсальных множествах $U_{КВК}\in\{0, max_{КВК}\}$ и $U_{ВВК}\in\{0, max_{ВВК}\}$ при $max_{КВК}$=512 и $max_{ВВК}$=300 и инициироваться экспертом на конкретных интервалах регистрации событий (ИРС) (например, N_{11}^i ($i=\overline{1,5}$) и N_{12}^j ($j=\overline{1,3}$) на ИРС [0; 2], [3, 8], [9; 16], [17; 128], [129; 512] и [0; 10], [11; 100], [101; 300] соответственно), (см. табл. 1 и табл. 2) для нечетких термов $T_{КВК}$ и $T_{ВВК}$.

Таблица 1

Данные для T_{KBK}

Значения ЛП	Интервал				
	N1	N2	N3	N4	N5
ОМ	7	3	1	0	0
М	2	5	2	0	0
С	1	2	7	1	0
Б	0	0	3	6	2
ОБ	0	0	2	4	5

Таблица 2

Данные для T_{BBK}

Значения ЛП	Интервал		
	N1	N2	N3
М	5	3	2
СР	2	4	1
СТ	0	3	4

На основе данных табл. 1 и табл. 2 формируется матрица подсказок (см. [2]) $\|k_j\| = \left\| \bigcup_{j=1}^{5} \sum_{i=1}^{5} b_{ij} \right\| = \|10,10,15,11,7\|$ и $\|k_j\| = \left\| \bigcup_{j=1}^{3} \sum_{i=1}^{3} b_{ij} \right\| = \|7,10,7\|$, а также, основываясь на выражении (1) в [2] при $i,j = \overline{1,5}$ и $i,j = \overline{1,3}$, определим $km = \bigvee_{j=1}^{5} k_j = 15$, $km = \bigvee_{j=1}^{3} k_j = 10$ и соответственно

$$\|c_{ij}\| = \begin{Vmatrix} 10,5 & 4,5 & 1 & 0 & 0 \\ 3 & 7,5 & 2 & 0 & 0 \\ 1,5 & 3 & 7 & 1,4 & 0 \\ 0 & 0 & 3 & 8,2 & 4,3 \\ 0 & 0 & 2 & 5,5 & 10,7 \end{Vmatrix}$$

$$\|c_{ij}\| = \begin{Vmatrix} 7,1 & 3 & 1,4 \\ 2,9 & 4 & 1,4 \\ 0 & 3 & 5,7 \end{Vmatrix}.$$

По выражению (2) в [2] $(i,j = \overline{1,5})$ при $cm_i = \bigcup_{j=1}^{5} \bigvee_{i=1}^{5} c_{ij} = \{10,5;\ 7,5;\ 7;\ 8,2;\ 10,7\}$ и $cm_i = \bigcup_{j=1}^{3} \bigvee_{i=1}^{3} c_{ij} = \{7,1;\ 4;\ 5,7\}$, вычисляем матрицы функций принадлежности, которые имеют следующий вид:

$$\|\mu_{ij}\| = \begin{Vmatrix} 1 & 0,43 & 0,1 & 0 & 0 \\ 0,4 & 1 & 0,27 & 0 & 0 \\ 0,2 & 0,43 & 1 & 0,2 & 0 \\ 0 & 0 & 0,37 & 1 & 0,52 \\ 0 & 0 & 0,19 & 0,5 & 1 \end{Vmatrix}$$

и

$$\|\mu_{ij}\| = \begin{Vmatrix} 1 & 0,42 & 0,2 \\ 0,7 & 1 & 0,35 \\ 0 & 0,5 & 1 \end{Vmatrix}.$$

Далее, получив оценочные соотношения для $\bigcup_{i=1}^{5} \Delta B_i / B = \{0,004;\ 0,016;\ 0,031;\ 0,125;\ 1\}$ и $\bigcup_{i=1}^{3} \Delta B_i / B = \{0,03;\ 0,33;\ 1\}$, формируются функции принадлежности НЧ. Так, например, для $\underset{\sim}{T}_{KBK} = \{\underset{\sim}{OM}, \underset{\sim}{M}, \underset{\sim}{C}, \underset{\sim}{Б}, \underset{\sim}{ОБ}\}$: $\underset{\sim}{OM} = \{1/0,004;$ $0,43/0,016;$ $0,1/0,031;$ $0/0,125;$ $0/1\}$; $\underset{\sim}{M} = \{0,4/0,004;$ $1/0,016;$ $0,27/0,031;$ $0/0,125;$ $0/1\}$; $\underset{\sim}{C} = \{0,2/0,004;$ $0,43/0,016;$ $1/0,031;$ $0,2/0,125;$ $0/1\}$; $\underset{\sim}{Б} = \{0/0,004;$ $0/0,016;$ $0,37/0,031;$ $1/0,125;$ $0,52/1\}$; $\underset{\sim}{ОБ} = \{0/0,004;$ $0/0,016;$ $0,19/0,031;$ $0,5/0,125;$ $1/1\}$, а для $\underset{\sim}{T}_{BBK} = \{\underset{\sim}{M}, \underset{\sim}{CP}, \underset{\sim}{CT}\}$: $\underset{\sim}{M} = \{1/0,03;$ $0,42/0,33;$ $0,2/1\}$; $\underset{\sim}{CP} = \{0,7/0,03;$ $1/0,33;$ $0,35/1\}$; $\underset{\sim}{CT} = \{0/0,03;$ $0,5/0,33;$ $1/1\}$.

Таким образом, на выходе УФЭ$_i$ БФЭ сформируется массив (вектор) T_{ij}^{ef}, например, при известных значениях n, j' и f' получим:

$$\text{УФЭ}_1(\{\underset{\sim}{T}_{KBK}^{e1}, \underset{\sim}{T}_{KBK}^{e2}, \underset{\sim}{T}_{KBK}^{e3}, \underset{\sim}{T}_{KBK}^{e4}, \underset{\sim}{T}_{KBK}^{e5}\},$$

$$\{\underset{\sim}{T}_{BBK}^{e1}, \underset{\sim}{T}_{BBK}^{e2}, \underset{\sim}{T}_{BBK}^{e3}\}) =$$

$$\text{УФЭ}_1(\{\underset{\sim}{OM}^e, \underset{\sim}{M}^e, \underset{\sim}{C}^e, \underset{\sim}{Б}^e, \underset{\sim}{ОБ}^e\}, \{\underset{\sim}{M}^e, \underset{\sim}{CP}^e, \underset{\sim}{CT}^e\})\ [2].$$

Далее, сформированные наборы НЧ для всех T_{ij}^{ef} перезаписываются в РЭ, при этом значения эталонов соответствующие параметрам i-й атаки заносятся в соответствующий регистр эталонов i-й атаки (РЭА$_i$) и хранятся там в течении всего вычислительного процесса (см. вершины 13–16 и 17 на рис. 2). Например, для $\underset{\sim}{T}_{KBK}^{e}$ и $\underset{\sim}{T}_{BBK}^{e}$ соответственно образуются $\underset{\sim}{T}_{KBK}^{e} = \bigcup_{i=1}^{5} \underset{\sim}{T}_{KBK}^{ei} = \{\underset{\sim}{T}_{KBK}^{e1}, \underset{\sim}{T}_{KBK}^{e2}, \ldots, \underset{\sim}{T}_{KBK}^{e5}\} = \{\underset{\sim}{OM}^e, \underset{\sim}{M}^e, \underset{\sim}{C}^e, \underset{\sim}{Б}^e, \underset{\sim}{ОБ}^e\}$, где $\underset{\sim}{OM}^e = \{0/0,004;$ $1/0,004;$ $0,43/0,016;$

0,1/0,031; 0/0,125}; $\underset{\sim}{M}^e$ ={0/0,004; 0,4/0,004; 1/0,016; 0,27/0,031; 0/0,125}; $\underset{\sim}{C}^e$ ={0/0,004; 0,2/0,004; 0,43/0,016; 1/0,031; 0,2/0,125; 0/1}; $\underset{\sim}{Б}^e$ ={0/0,016; 0,37/0,031; 1/0,125; 0,52/1; 0/1}; $\underset{\sim}{ОБ}^e$ ={0/0,016; 0,19/0,031; 0,5/0,125; 1/1; 0/1} и $\underset{\sim}{T}^e_{ВВК} = \bigcup_{i=1}^{3} \underset{\sim}{T}^{ei}_{ВВК} = \{ \underset{\sim}{T}^{e1}_{ВВК}, \underset{\sim}{T}^{e2}_{ВВК}, \underset{\sim}{T}^{e3}_{ВВК} \} = \{ \underset{\sim}{M}^e, \underset{\sim}{CP}^e, \underset{\sim}{CT}^e \}$, где $\underset{\sim}{M}^e$ ={0/0,03; 1/0,03; 0,42/0,33; 0,2/1; 0/1}; $\underset{\sim}{CP}^e$ ={0/0,03; 0,7/0,03; 1/0,33; 0,35/1; 0/1}; $\underset{\sim}{CT}^e$ ={0/0,03; 0,5/0,33; 1/1; 0/1}.

И, наконец, для каждого T^{ef}_{ij} посредством сопроцессоров визуализации ($СВ_i$, $i = \overline{1,n}$) в ПВЭ формируется графическое изображение эталонов параметров для каждой AT_i. Другими словами, $СВ_1$ визуализирует эталон для AT_1, $СВ_2$ – для AT_2, а $СВ_n$ – для AT_n, например, при $n=3$ $СВ_1$ визуализирует эталоны для *SN (CBSN)*, $СВ_2$ – для *DS (CBDS)*, а $СВ_3$ – *SP (CBSP)* [2] (см. вершины 13–15 и 18 на рис. 2).

Например, полученные эталонные значения для ЛП КВК и ВВК, соответственно визуализированы в виде графиков на рис. 3 и рис. 4.

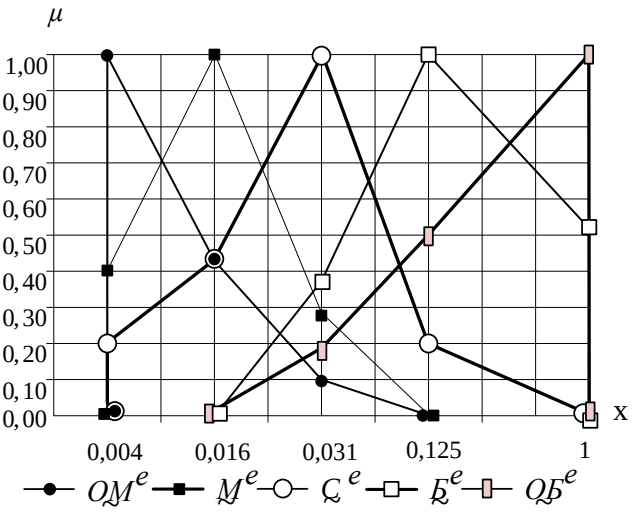

Рис. 3. Эталонные НЧ для КВК

Разработанная структура системы формирования НЭ сетевых параметров (см. рис. 1) может быть реализована программно или программно-аппаратно и ориентирована на измерение текущих значений параметров сетевого трафика с целью идентификации аномального состояния, а также может использоваться в системах выявления аномального состояния, реализующих соответствующий метод [4].

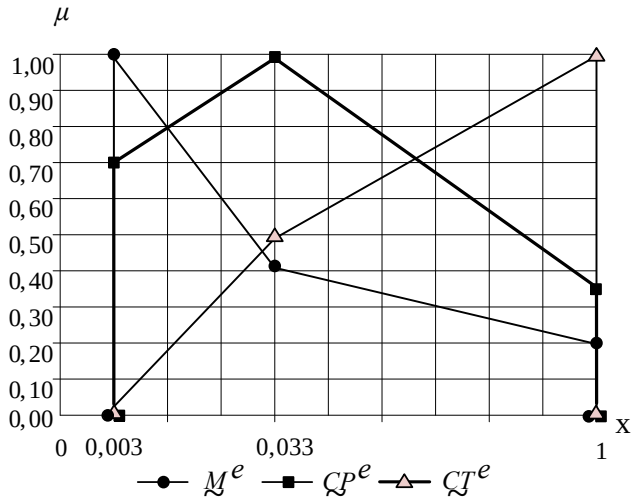

Рис. 4. Эталонные НЧ для ВВК

ЛИТЕРАТУРА

[1]. 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.

[2]. Модели эталонов лингвистических переменных для систем выявления атак / М.Г. Луцкий, А.А. Корченко, А.В. Гавриленко, А.А Охрименко // Захист інформації. – 2012. – № 2 (55). – С. 71-78.

[3]. Корченко А.А. Модель эвристических правил на логико-лингвистических связках для обнаружения аномалий в компьютерных системах / А.А. Корченко // Захист інформації. – 2012. – № 4 (57). – С. 112-118.

[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.А. Модели систем выявления аномалий, порожденных кибератаками / А.А. Корченко // Эвристические алгоритмы и распределенные вычисления в прикладных задачах : Коллективная монография / Под ред. Б.Ф. Мельникова. – Ульяновск, 2013. – Выпуск 2. – С. 56-86.

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

[7]. Корченко А.Г. Построение систем защиты информации на нечетких множествах [Текст] : Тео-

рия и практические решения / А.Г. Корченко. – К. : МК-Пресс, 2006. – 320 с.

[8]. Горніцька Д.А. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки / Д.А. Горніцька, В.В. Волянська, А.О. Корченко // Захист інформації. – 2012. – №1 (54). – С. 108-121.

REFERENCES

[1]. 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.

[2]. 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.

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

[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.A. The system models of anomaly detection caused by cyber-attacks, heuristic algorithms and distributed computing applications, Ulianovsk, 2013, V 2, pp. 56-86.

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

[7]. Korchenko A.G. The development of information protection systems based on the fuzzy sets, The theory and practical solutions, Kuev, 2006, 320 p.

[8]. Hornitska D.A., Volyanskaya V.V., Korchenko A.A. Weight numbers defining for expert evaluation in the information security sphere, Zahist ìnformacìï, 2012, №1 (54), pp. 108-121.

СИСТЕМА ФОРМУВАННЯ НЕЧІТКИХ ЕТАЛОНІВ МЕРЕЖЕВИХ ПАРАМЕТРІВ

На основі відомого методу виявлення аномалій породжених кібератаками розроблена відповідна система, для підтримки функціонування якої необхідна реалізація засобу формування нечітких еталонів, орієнтованого на вимірювання поточних значень параметрів мережевого трафіку з метою виявлення підозрілої активності в середовищі оточення. Для вирішення такого завдання запропоновано нове структурне рішення відповідної системи, що складається з регістра еталонів, атак і параметрів, а також блоків комутації параметрів, зв'язування атаки з параметром, формування сукупності термів, формування еталонів, регістра еталонів і процесора візуалізації еталонів. Ця розробка може бути реалізована програмно або програмно-апаратно і орієнтована на вимірювання поточних значень параметрів мережевого трафіку з метою ідентифікації аномального стану.

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

THE SYSTEM DEVELOPMENT OF FUZZY STANDARDS OF NETWORK PARAMETERS

Based on the well-known anomaly detection techniques caused by the cyber –attacks, it was developed an appropriate system which requires the implementation of fuzzy standards focused on the measurement of current parameter value of the network traffic in order to identify suspicious activity in the Environment. To solve this task it was suggested a new structural decision of the corresponding system, consisting of the register of standards, attacks and parameters, as well as blocks of switching parameters, linking the attack to the parameter, the development of set of terms, the development of standards, register of standards and the processor of standards visualization. This development can be implemented through the software or firmware, hardware and focused on the measurement of current values of parameters in the network traffic in order to identify an abnormal condition.

Index Terms: cyber attacks, anomalies, intrusion detection systems, anomaly detection systems, attack detection, anomaly detection in computer networks, fuzzy standards.

Корченко Анна Александровна, кандидат технических наук, доцент кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: annakor@ukr.net

Корченко Анна Олександрівна, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Anna Korchenko PhD in Eng., Associate Professor of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).