© Korchenko A. Method of parameter fuzzification based on linguistic standards for cyber attacks detection // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 1, p. 21-28.

МЕТОД ФАЗЗИФИКАЦИИ ПАРАМЕТРОВ НА ЛИНГВИСТИЧЕСКИХ ЭТАЛОНАХ ДЛЯ СИСТЕМ ВЫЯВЛЕНИЯ КИБЕРАТАК

Анна Корченко

Национальный авиационный университет, Украина

КОРЧЕНКО Анна Александровна, к.т.н.

Год и место рождения: 1985 год, г. Киев, Украина.
Образование: Национальный авиационный университет, 2007 год.
Должность: доцент кафедры безопасности информационных технологий.
Научные интересы: информационная безопасность, системы обнаружения вторжений, экспертное оценивание в сфере защиты информации.
Публикации: больше 30 научных публикаций, среди которых научные статьи, учебники и учебно-методические пособия.
E-mail: annakor@ukr.net

Аннотация. *Одной из базовых задач в области информационной безопасности является создание систем защиты сетевых и системных ресурсов, основанных на аномальном принципе. Для построения и расширения функциональности такого рода систем используется метод выявления аномалий, порожденных кибератаками в информационных системах. В этом методе процесс фаззификации параметров практически не формализован, что понижает эффективность его использования. С этой целью предлагается метод, который базируется на лингвистических эталонах, математических моделях, методах нечеткой логики и реализуется посредством трех основных этапов: формирование частот встречаемости параметров; формирование поправочных эталонов; формирование нечетких параметров. Посредством этих этапов осуществляется фаззификация текущих значений величин при решении задач выявления кибератак в компьютерных системах, что повысит эффективность построения соответствующих систем обнаружения вторжений.*

Ключевые слова: *кибератаки, аномалии, нечеткие эталоны, лингвистические эталоны, метод фаззификации параметров, фаззификация параметров, системы обнаружения вторжений, системы обнаружения аномалий, системы обнаружения атак, обнаружение аномалий в компьютерных сетях.*

Актуальность

Стремительное развитие информационных технологий в свою очередь породило большое количество угроз ресурсам информационных систем. Известным решением обеспечения безопасности таких ресурсов, являются системы обнаружения вторжений. Одной из базовых задач в области информационной безопасности является создание систем защиты сетевых и системных ресурсов, которые позволяют анализировать, контролировать, прогнозировать и блокировать несигнатурные, а также новые типы кибератак. Одним из решений таких задач является использование соответствующих систем обнаружения вторжений, которые основаны на программных или программно-аппаратных реализациях и ориентированы на установление фактов несанкционированного доступа через компьютерные сети.

Анализ существующих исследований

Для построения и расширения функциональности такого рода систем [1-3] используется метод выявления аномалий, порожденных кибератаками в информационных системах [4]. В этом методе процесс фаззификации параметров практически не формализован, что понижает эффективность его использования. Для эффективного применения метода выявления аномалий необходима формальная реализация этапа 5 – фаззификация параметров [4], посредством которого формируются требуемые для последующих вычислений текущие значения нечетких параметров в моделируемой среде окружения. Исходя из этого, создание методов, позволяющих фаззифировать текущие значения параметров для систем выявления кибератак, есть актуальной задачей.

Основная цель исследования

Целью данной работы является разработка метода фаззификации параметров на лингвистических эталонах (МФПЛЭ), позволяющего сформировать текущие значения переменных в нечеткой форме, посредством которых формализуются параметры характерные для конкретной среды окружения при решении задач выявления кибератак в компьютерных системах.

Основная часть исследования

Основу предлагаемого метода составляют три базовых этапа: формирование частот встречаемости параметров; формирование поправочных эталонов; формирование нечетких параметров.

Этап 1 – формирование частот встречаемости параметров. Для реализации этого этапа введем множество всех возможных сенсоров **S** и подмножества таких сенсоров $\mathbf{S_{ij}} \in \mathbf{S}$:

$$\mathbf{S_{ij}} = \bigcup_{k=1}^{r} S_{ijk}(t_\eta) = \{ S_{ij1}(t_\eta),\ S_{ij2}(t_\eta),\ \ldots,\ S_{ijr}(t_\eta) \}, \quad (1)$$

используемых для контроля текущего состояния физических параметров, определяемых посредством множества пар $\mathbf{AT \rightarrow P_n}$ [5].

Здесь $S_{ijk}(t_\eta)$ $(i = \overline{1,n},\ j = \overline{1,m},\ k = \overline{1,r})$ является сенсором N_{ijk}-го интервала [6], отражающем значение (на соответствующем интервале) физического параметра $P_{ij}(t_\eta)$ в момент t_η, а r – количество сенсоров.

Сенсор $S_{ijk}(t_\eta)$ представляет собой бинарную функцию, которая эквивалентна единице только в случае, когда значение $P_{ij}(t_\eta)$ относительно множества $\mathbf{AT \rightarrow P_n}$ в момент t_η (момент наступления ожидаемого события) будет находиться в интервале N_{ijk} т.е.:

$$S_{ijk}(t_\eta) = \begin{cases} 1, \text{ при } P_{ij}(t_\eta) \in N_{ijk} \\ 0, \text{ при } P_{ij}(t_\eta) \notin N_{ijk} \end{cases} \quad (2)$$
$$(k = \overline{1,r}).$$

Далее, введем множество всех возможных счетчиков сенсоров **CS** и подмножества таких счетчиков $\mathbf{CS_{ij}} \in \mathbf{CS}$, которые согласно выражения (3), на основе данных сенсоров $S_{ijk}(t_\eta)$, характеризующих текущее состояние *j*-х физических параметров относительно *i*-й атаки в моменты t_η, формируются частоты встречаемости значений $P_{ij}(t_\eta)$ на каждом из интервалов N_{ijk} $(k = \overline{1,r})$ [6] посредством подмножеств

$$\mathbf{CS_{ij}} = \bigcup_{k=1}^{r} CS_{ijk} = \bigcup_{k=1}^{r} \sum_{\eta=1}^{\eta_{max}} S_{ijk}(t_\eta), \quad (3)$$

где CS_{ijk} является счетчиком сенсора $S_{ijk}(t_\eta)$, а η_{max} соответствует общему количеству возможных t_η.

Далее, указанные частоты встречаемости, отображаемые счетчиками CS_{ijk} $(k = \overline{1,r})$ представим в виде таблицы (табл. 1).

Таблица 1

Типовая таблица для $\mathbf{CS_{ij}}$

Счетчик сенсора	$\mathbf{N_{ij}}$ $(k = \overline{1,r})$			
	N_{ij1}	N_{ij2}	…	N_{ijr}
CS_{ij}	CS_{ij1}	CS_{ij2}	…	CS_{ijk}

Например, для реализации этапа формирования частот встречаемости параметров при $i = 3$ ($\mathbf{AT_i = AT_3 = AT_{SP}}$), $j = 3$ ($\mathbf{P_{ij} = P_{33} \in P_{SPKOП}}$) (т.е. AT_3=*SP* – «Спуфинг», P_3=*КОП* – «Количество одновременных подключений к серверу») и $r = 5$ подмножество $\mathbf{S_{ij} = S_{33}}$ согласно выражения (1) принимает вид

$$\mathbf{S_{33}} = \bigcup_{k=1}^{5} S_{33k}(t_\eta) = \{ S_{331}(t_\eta),\ S_{332}(t_\eta),$$
$$S_{333}(t_\eta),\ S_{334}(t_\eta),\ S_{335}(t_\eta) \} =$$
$$\{ S_{SPKOП1}(t_\eta),\ S_{SPKOП2}(t_\eta),\ S_{SPKOП3}(t_\eta),$$
$$S_{SPKOП4}(t_\eta),\ S_{SPKOП5}(t_\eta) \},$$

где $S_{331}(t_\eta) = S_{SPKOП1}(t_\eta)$, $S_{332}(t_\eta) = S_{SPKOП2}(t_\eta)$, $S_{333}(t_\eta) = S_{SPKOП3}(t_\eta)$, $S_{334}(t_\eta) = S_{SPKOП4}(t_\eta)$ и $S_{335}(t_\eta) = S_{SPKOП5}(t_\eta)$, соответственно сенсоры интервалов $N_{ij1} = N_{331} = N_{SPKOП1}$, $N_{ij2} = N_{332} = N_{SPKOП2}$, $N_{ij3} = N_{333} = N_{SPKOП3}$, $N_{ij4} = N_{334} = N_{SPKOП4}$ и $N_{ij5} = N_{335} = N_{SPKOП5}$, которые используются для контроля текущего состояния параметра $P_{SPKOП}(t_\eta)$ (относительно множества $\mathbf{AT \rightarrow P_n}$) в моменты t_η при $r = 5$.

Поскольку сенсоры $S_{33k}(t_\eta)$ $(k = \overline{1,r})$ исходя из выражения (2) определяются как

$$S_{33k}(t_\eta) = S_{SPKOПk}(t_\eta) =$$
$$\begin{cases} 1, \text{ при } P_{33}(t_\eta) \in N_{33k} \\ 0, \text{ при } P_{33}(t_\eta) \notin N_{33k} \end{cases} (k = \overline{1,5}),$$

то частоты встречаемости значений $P_{33}(t_\eta)$ согласно формулы (3) сформируем посредством следующего выражения

$$\mathbf{CS_{33}} = \bigcup_{k=1}^{5} CS_{33k} = \bigcup_{k=1}^{5} \sum_{\eta=1}^{\eta_{max}} S_{33k}(t_\eta) =$$

$$\{\sum_{\eta=1}^{\eta_{max}} S_{331}(t_\eta), \sum_{\eta=1}^{\eta_{max}} S_{332}(t_\eta), \sum_{\eta=1}^{\eta_{max}} S_{333}(t_\eta),$$

$$\sum_{\eta=1}^{\eta_{max}} S_{334}(t_\eta), \sum_{\eta=1}^{\eta_{max}} S_{335}(t_\eta)\} =$$

$$\{\sum_{\eta=1}^{\eta_{max}} S_{SPKOP1}(t_\eta), \sum_{\eta=1}^{\eta_{max}} S_{SPKOP2}(t_\eta),$$

$$\sum_{\eta=1}^{\eta_{max}} S_{SPKOP3}(t_\eta), \sum_{\eta=1}^{\eta_{max}} S_{SPKOP4}(t_\eta),$$

$$\sum_{\eta=1}^{\eta_{max}} S_{SPKOP5}(t_\eta)\}.$$

Для инициирования сенсоров им необходимо получить текущие значения $P_{DSKOP}(t_\eta)$, $P_{SPKOP}(t_\eta)$, $P_{DSCO3}(t_\eta)$, $P_{DS3M3}(t_\eta)$ и $P_{SPKPOA}(t_\eta)$.

Пример формирования $P_{DSKOP}(t_\eta)$ и $P_{SPKOP}(t_\eta)$ соответственно для сенсоров CS_{23} и CS_{33} может основываться на использовании веб-сервера с известной конфигурацией [7], подключения к которому преимущественно осуществляются по порту 80/tcp. В этом случае посредством утилиты netstat с параметрами: netstat -plan | grep :80 | awk '{print $10}' | cut -d: -f1 | sort | sort -n была произведена фиксация количества подключений, а t_η интерпретируется как время $(\eta = \overline{1,60})$, где момент $t_1 = 1$с, $t_2 = 2$с, …, $t_{60} =$ 60с, т.е. интервал дискретизации времени соответствует одной секунде (табл. 2).

Для получения $P_{SPKPOA}(t_\eta)$ использовалась информация генерируемая Iptables, а значения $P_{DSCO3}(t_\eta)$ формировались посредством анализа логов веб-сервера, путем подсчета количества всех запросов за указанные моменты t_η $(\eta = \overline{1,60})$.

При формировании $P_{DS3M3}(t_\eta)$ использовалась методика измерения, основанная на создании потока для каждого уникального по IP-адресу подключения. Мониторинг осуществляется путем подсчета количества полученных от клиента запросов определенного типа (в данном случае GET-запросов) за выше принятые временные интервалы с последующим вычислением среднего времени между последовательными запросами и занесением (для удобства отображения данных) результатов в табл. 2, из которой, например, видно, что после 30-й секунды осуществляется уменьшение задержки, что при большом количестве подключений может свидетельствовать о начальных атакующих действиях.

Следует отметить, что для разных атак $i = \overline{2,3}$ значения частот встречаемости текущего состояния параметров может быть одинаковым. Так, например, в сформированной табл. 2 $P_{23}(t_\eta) = P_{33}(t_\eta) = P_{DSKOP}(t_\eta) = P_{SPKOP}(t_\eta)$, при этом значения сенсоров $S_{331} = S_{SPKOP1}$, $S_{332} = S_{SPKOP2}$, $S_{333} = N_{SPKOP3}$, $S_{334} = S_{SPKOP4}$ и $S_{335} = S_{SPKOP5}$ для $P_{SPKOP}(t_\eta)$ попадают в соответствующие интервалы $N_{331} = N_{SPKOP1}$ <=> *[0; 8]*, $N_{332} = N_{SPKOP2}$ <=> *[9; 64]*, $N_{333} = N_{SPKOP3}$ <=> *[65; 256]*, $N_{334} = N_{SPKOP4}$ <=> *[257; 512]* и $N_{335} = N_{SPKOP5}$ <=> *[513; 1024]* [6], а отмеченные светло-серым маркером значения $P_{SPKOP}(t_1) = 17$, $P_{SPKOP}(t_2) = 19$, $P_{SPKOP}(t_3) = 30$, $P_{SPKOP}(t_{44}) = 41$, $P_{SPKOP}(t_{45}) = 51$ и $P_{SPKOP}(t_{47}) = 26$ попадают в интервал $N_{332} = N_{SPKOP2}$ <=> *[9; 64]*.

Таблица 2

Значения физических параметров $P_{DSKOP}(t_\eta) = P_{SPKOP}(t_\eta)$ и их сенсоров при t_η $(\eta = \overline{1,60})$

t_η $(\eta = \overline{1,60})$	$P_{DSKOP}(t_\eta) = P_{SPKOP}(t_\eta)$	$P_{DSCO3}(t_\eta)$	$P_{DS3M3}(t_\eta)$	$P_{SPKPOA}(t_\eta)$	$S_{231} = S_{331}$	$S_{232} = S_{332}$	$S_{233} = S_{333}$	$S_{234} = S_{334}$	$S_{235} = S_{335}$
1; 31	17; 234	87; 79	154; 80	82; 536	0; 0	1; 0	0; 1	0; 0	0; 0
2; 32	19; 234	80; 95	203; 74	89; 512	0; 0	1; 0	0; 1	0; 0	0; 0
3; 33	30; 180	86; 91	217; 72	95; 562	0; 0	1; 0	0; 1	0; 0	0; 0
4; 34	102; 266	101; 89	183; 92	92; 559	0; 0	0; 0	1; 0	0; 1	0; 0
5; 35	70; 195	82; 92	146; 128	96; 541	0; 0	0; 0	1; 1	0; 0	0; 0
6; 36	258; 193	86; 89	151; 93	88; 519	0; 0	0; 0	0; 1	1; 0	0; 0
7; 37	225; 208	95; 86	142; 86	86; 559	0; 0	0; 0	1; 1	0; 0	0; 0
8; 38	294; 279	99; 99	149; 94	81; 527	0; 0	0; 0	0; 0	1; 1	0; 0
9; 39	181; 283	86; 86	191; 89	99; 549	0; 0	0; 0	1; 0	0; 1	0; 0

Окончание таблицы 2

10; 40	205; 161	100; 98	163; 41	88; 514	0; 0	0; 0	1; 1	0; 0	0; 0
11; 41	170; 161	85; 95	150; 51	99; 541	0; 0	0; 0	1; 1	0; 0	0; 0
12; 42	253; 81	85; 87	215; 35	85; 360	0; 0	0; 0	1; 1	0; 0	0; 0
13; 43	281; 74	79; 100	185; 39	524; 357	0; 0	0; 0	0; 1	1; 0	0; 0
14; 44	164; 41	81; 59	148; 38	539; 357	0; 0	0; 1	1; 0	0; 0	0; 0
15; 45	208; 51	85; 54	145; 46	543; 350	0; 0	0; 1	1; 0	0; 0	0; 0
16; 46	247; 158	82; 51	141; 90	518; 365	0; 0	0; 0	1; 1	0; 0	0; 0
17; 47	125; 26	87; 65	163; 40	542; 359	0; 0	0; 1	1; 0	0; 0	0; 0
18; 48	266; 235	100; 51	168; 60	551; 344	0; 0	0; 0	0; 1	1; 0	0; 0
19; 49	273; 198	87; 64	137; 38	540; 345	0; 0	0; 0	0; 1	1; 0	0; 0
20; 50	285; 178	84; 55	147; 82	541; 367	0; 0	0; 0	0; 1	1; 0	0; 0
21; 51	230; 167	94; 51	123; 54	554; 345	0; 0	0; 0	1; 1	0; 0	0; 0
22; 52	141; 114	92; 51	139; 33	540; 345	0; 0	0; 0	1; 1	0; 0	0; 0
23; 53	79; 253	84; 68	160; 44	537; 363	0; 0	0; 0	1; 1	0; 0	0; 0
24; 54	205; 276	86; 69	143; 57	554; 346	0; 0	0; 0	1; 0	0; 1	0; 0
25; 55	113; 160	80; 61	171; 39	543; 347	0; 0	0; 0	1; 1	0; 0	0; 0
26; 56	175; 289	90; 55	82; 51	532; 358	0; 0	0; 0	1; 0	0; 1	0; 0
27; 57	144; 163	84; 57	94; 60	564; 367	0; 0	0; 0	1; 1	0; 0	0; 0
28; 58	168; 174	94; 55	127; 28	511; 367	0; 0	0; 0	1; 1	0; 0	0; 0
29; 59	169; 174	87; 67	69; 56	563; 356	0; 0	0; 0	1; 1	0; 0	0; 0
30; 60	288; 174	86; 48	103; 33	539; 540	0; 0	0; 0	0; 1	1; 0	0; 0

Согласно выражения (2) сенсор $S_{332}(t_\eta)$ определяется как

$$S_{332}(t_\eta) = S_{SPKOП2}(t_\eta) = \begin{cases} 1, \text{ при } P_{SPKOП2}(t_\eta) \in N_{SPKOП2} \\ 0, \text{ при } P_{SPKOП2}(t_\eta) \notin N_{SPKOП2} \end{cases} (\eta = \overline{1,60}).$$

Очевидно, что в моменты времени t_1, t_2, t_3, t_{44}, t_{45} и t_{47} значения $S_{332}(t_1) = S_{332}(t_2) = S_{332}(t_3) = S_{332}(t_{44}) = S_{332}(t_{45}) = S_{332}(t_{47})$=1, а в оставшееся время соответственно равны 0. Для удобства восприятия заносим в табл. 2 сформированные в указанные моменты времени состояния сенсоров S_{331}, S_{332}, S_{333}, S_{334} и S_{335}.

Далее, при $i = \overline{2,3}$, $j = \overline{3,6}$ определим CS_{3j} для $P_{33}(t_\eta) = P_{SPKOП}(t_\eta)$ и $P_{36}(t_\eta) = P_{SPKПОА}(t_\eta)$ на множестве $\mathbf{N_{33}}$ $(r = 5)$ и $\mathbf{N_{36}}$ $(r = 3)$ (табл. 3), а также CS_{2j} для $P_{23}(t_\eta) = P_{DSKOП}(t_\eta)$, $P_{24}(t_\eta) = P_{DSCO3}(t_\eta)$ и $P_{25}(t_\eta) = P_{DS3M3}(t_\eta)$ на $\mathbf{N_{23}}$ $(r = 5)$, $\mathbf{N_{24}}$ $(r = 3)$ и $\mathbf{N_{25}}$ (при $r = 3$) (табл. 4).

Например, значение счетчика сенсоров CS_{332} согласно выражения (3) соответствует $CS_{SPKOП2} = 6$ (см. табл. 3), а все оставшиеся CS_{3j} и CS_{2j} определены аналогичным способом и занесены соответственно в табл. 3 и табл. 4.

Таблица 3

Частоты встречаемости текущего состояния параметров $P_{SPKOП}(t_\eta)$ и $P_{SPKПОА}(t_\eta)$

CS_{ij}	$\mathbf{N_{33}}$ $(r = 5,\ j = 3)$					$\mathbf{N_{36}}$ $(r = 3,\ j = 6)$		
	N_{331}	N_{332}	N_{333}	N_{334}	N_{335}	N_{361}	N_{362}	N_{363}
CS_{3j}	0	6	42	12	0	0	12	48

Таблица 4

Частоты встречаемости текущего состояния параметров $P_{DSKOП}(t_\eta)$, $P_{DSCO3}(t_\eta)$ и $P_{DS3M3}(t_\eta)$

CS_{ij}	$\mathbf{N_{23}}$ $(r = 5,\ j = 3)$					$\mathbf{N_{24}}$ $(r = 3,\ j = 4)$			$\mathbf{N_{25}}$ $(r = 3,\ j = 5)$		
	N_{231}	N_{232}	N_{233}	N_{234}	N_{235}	N_{241}	N_{242}	N_{243}	N_{251}	N_{252}	N_{253}
CS_{2j}	0	6	42	12	0	0	60	0	0	32	28

Таким образом формируются все частоты встречаемости текущих параметров, отображаемые подмножествами счетчиков сенсоров $\mathbf{CS_{ij}} \in \mathbf{CS}$.

Этап 2 – формирование поправочных эталонов. Для реализации этого этапа введем подмножества поправочных эталонов $\mathbf{T^E_{ij}} \in \mathbf{T^E}$, ($\mathbf{T^E}$ – множество всех возможных поправочных эталонов), каждое из которых основывается на $\mathbf{T^e_{ij}}$ [6] и определяется как

$$\mathbf{T^E_{ij}} = \bigcup_{s=1}^{r} \underset{\sim}{T}^E_{ijs} = \{\underset{\sim}{T}^E_{ij1},\ \underset{\sim}{T}^E_{ij2}, \ldots,\ \underset{\sim}{T}^E_{ijs}, \ldots,\ \underset{\sim}{T}^E_{ijr}\}, \quad (4)$$

где $\underset{\sim}{T}^E_{ijs}$ $(s=\overline{1,r})$ - поправочные эталонные нечеткие числа (НЧ). Эти числа строятся на основе преобразования соответствующих НЧ (см. (12) в [6]) из подмножества $\mathbf{T^e_{ij}} \in \mathbf{T^e}$ с помощью счетчиков сенсоров из $\mathbf{CS_{ij}} \in \mathbf{CS}$, согласно выражения

$$\bigcup_{s=1}^{r} \underset{\sim}{T}^E_{ijs} = \bigcup_{s=1}^{r} (\underset{\sim}{T}^e_{ijs} \cdot CS_{ijs}) = \{\underset{\sim}{T}^e_{ij1} \cdot CS_{ij1},\ \underset{\sim}{T}^e_{ij2} \cdot CS_{ij2}, \ldots,\ \underset{\sim}{T}^e_{ijr} \cdot CS_{ijr}\}. \quad (5)$$

Например, для $i=j=3$ согласно выражений (4) и (5) поправочные эталоны определяются как

$$\mathbf{T^E_{33}} = \bigcup_{s=1}^{5} \underset{\sim}{T}^E_{33s} = \bigcup_{s=1}^{5} (\underset{\sim}{T}^e_{33s} \cdot CS_{33s}) = \{\underset{\sim}{T}^e_{331} \cdot CS_{331},\ \underset{\sim}{T}^e_{332} \cdot CS_{332},\ \underset{\sim}{T}^e_{333} \cdot CS_{333},\ \underset{\sim}{T}^e_{334} \cdot CS_{334},\ \underset{\sim}{T}^e_{335} \cdot CS_{335}\} = \{\underset{\sim}{OM}^E_{33},\ \underset{\sim}{M}^E_{33},\ \underset{\sim}{C}^E_{33},\ \underset{\sim}{B}^E_{33},\ \underset{\sim}{OB}^E_{33}\} <=> \mathbf{T^E_{SPKOP}} = \bigcup_{s=1}^{5} \underset{\sim}{T}^E_{SPKOP\,s} = \bigcup_{s=1}^{5} (\underset{\sim}{T}^e_{SPKOPs} \cdot CS_{SPKOPs})$$

$$= \{\underset{\sim}{T}^e_{SPKOP1} \cdot CS_{SPKOP1},\ \underset{\sim}{T}^e_{SPKOP2} \cdot CS_{SPKOP2},\ \underset{\sim}{T}^e_{SPKOP3} \cdot CS_{SPKOP3},\ \underset{\sim}{T}^e_{SPKOP4} \cdot CS_{SPKOP4},\ \underset{\sim}{T}^e_{SPKOP5} \cdot CS_{SPKOP5}\} = \{\underset{\sim}{T}^E_{SPKOP1},\ \underset{\sim}{T}^E_{SPKOP2},\ \underset{\sim}{T}^E_{SPKOP3},\ \underset{\sim}{T}^E_{SPKOP4},\ \underset{\sim}{T}^E_{SPKOP5}\}.$$

Таким образом, фактически осуществляется умножение эталонных НЧ $\underset{\sim}{OM}^e_{23}$, $\underset{\sim}{M}^e_{23}$, $\underset{\sim}{C}^e_{23}$, $\underset{\sim}{B}^e_{23}$ и $\underset{\sim}{OB}^e_{23}$ (см. пример этапа 5 в [6]), входящих в $\mathbf{T^e_{33}} = \mathbf{T^e_{SPKOP}}$ на значения CS_{331}, CS_{332}, CS_{333}, CS_{334} и CS_{335} соответственно. Отметим, что согласно выражений (4) и (5) $\underset{\sim}{T}^E_{331} = \underset{\sim}{T}^E_{SPKOP1} = \underset{\sim}{OM}^E_{33} = \underset{\sim}{OM}^e_{33} \cdot 0 = \{$ *0/0,008; 1/0,008; 0,25/0,063; 0/0,25* $\} \cdot 0 = \{$ *0/0; 1/0; 0,25/0; 0/0* $\}$, $\underset{\sim}{T}^E_{332} = \underset{\sim}{T}^E_{SPKOP2} = \underset{\sim}{M}^E_{33} = \underset{\sim}{M}^e_{33} \cdot 6 = \{$ *0/0,008; 0,67/0,008; 1/0,063; 0,33/0,25; 0/0,5* $\} \cdot 6 = \{$ *0/0,048; 0,67/0,048; 1/0,378; 0,33/1,5; 0/3* $\}$, $\underset{\sim}{T}^E_{333} = \underset{\sim}{T}^E_{SPKOP3} = \underset{\sim}{C}^E_{33} = \underset{\sim}{C}^e_{33} \cdot 42 = \{$ *0/0,008; 0,25/0,063; 1/0,25; 0,5 /0,5; 0/1* $\} \cdot 42 = \{$ *0/0,336; 0,25/ 2,646; 1/10,5; 0,5/21; 0/42* $\}$, $\underset{\sim}{T}^E_{334} = \underset{\sim}{T}^E_{SPKOP4} = \underset{\sim}{B}^E_{33} = \underset{\sim}{B}^e_{33} \cdot 12 = \{$ *0/0,063; 0,5/0,25; 1/0,5; 0,75/1; 0/1* $\} \cdot 12 = \{$ *0/0,756; 0,5/3; 1/6; 0,75/12; 0/12* $\}$, а $\underset{\sim}{T}^E_{335} = \underset{\sim}{T}^E_{SPKOP5} = \underset{\sim}{OB}^E_{33} = \underset{\sim}{OB}^e_{33} \cdot 0 = \{$ *0/0,25; 0,83/0,5; 1/1; 0/1* $\} \cdot 0 = \{$ *0/0; 0,83/0; 1/0; 0/0* $\}$.

По аналогии с $\mathbf{T^E_{33}}$ произведем вычисления для $\mathbf{T^E_{36}}$ при $i=3$ и $j=6$. Тогда согласно формул (4) и (5) $\mathbf{T^E_{36}} = \bigcup_{s=1}^{3} \underset{\sim}{T}^E_{36\,s} = \bigcup_{s=1}^{3} (\underset{\sim}{T}^e_{36s} \cdot CS_{36\,s}) = \{\underset{\sim}{T}^e_{361} \cdot CS_{361},\ \underset{\sim}{T}^e_{362} \cdot CS_{362},\ \underset{\sim}{T}^e_{363} \cdot CS_{363}\} = \{\underset{\sim}{M}^E_{36},\ \underset{\sim}{C}^E_{36},\ \underset{\sim}{B}^E_{36}\}$ <=> $\mathbf{T^E_{SPKPOA}} = \bigcup_{s=1}^{3} \underset{\sim}{T}^E_{SPKPOA\,s} = \bigcup_{s=1}^{3} (\underset{\sim}{T}^e_{SPKPOAs} \cdot CS_{SPKPOAs}) = \{\underset{\sim}{T}^e_{SPKPOA1} \cdot CS_{SPKPOA1},\ \underset{\sim}{T}^e_{SPKPOA2} \cdot CS_{SPKPOA2},\ \underset{\sim}{T}^e_{SPKPOA3} \cdot CS_{SPKPOA3}\} = \{\underset{\sim}{T}^E_{SPKPOA1},\ \underset{\sim}{T}^E_{SPKPOA2},\ \underset{\sim}{T}^E_{SPKPOA3}\}$, а соответствующие поправочные эталоны вычисляются по выражениям: $\underset{\sim}{T}^E_{361} = \underset{\sim}{T}^E_{SPKPOA1} = \underset{\sim}{M}^E_{36} = \underset{\sim}{M}^e_{36} \cdot 0 =$ *{0/0,01; 1/0,01; 0,33/0,1; 0/1}* $\cdot 0 =$ *{0/0; 1/0; 0,33/0; 0/0}*; $\underset{\sim}{T}^E_{362} = \underset{\sim}{T}^E_{SPKPOA2} = \underset{\sim}{C}^E_{36} = \underset{\sim}{C}^e_{36} \cdot 12 =$ *{0/0,01; 0,25/0,01; 1/0,1; 0,5/1; 0/1}* $\cdot 12 =$ *{0/0,12; 0,25/0,12; 1/1,2; 0,5/12; 0/12}*; $\underset{\sim}{T}^E_{363} = \underset{\sim}{T}^E_{SPKPOA3} = \underset{\sim}{B}^E_{36} = \underset{\sim}{B}^e_{36} \cdot 48 =$ *{0/0,01; 0,67/0,1; 1/1; 0/1}* $\cdot 48 =$ *{0/0,48; 0,67/4,8; 1/48; 0/48}*. Таким образом, формируются все подмножества поправочных эталонов $\mathbf{T^E_{ij}} \in \mathbf{T^E}$.

Этап 3 - формирование нечетких параметров. Реализация этого этапа осуществляется по следующему выражению

$$\underset{\sim}{P}_{ij} = (\sum_{s=1}^{r} \underset{\sim}{T}^E_{ijs}) / \eta_{max} = (\underset{\sim}{T}^E_{ij1} \tilde{+} \underset{\sim}{T}^E_{ij2} \tilde{+} \ldots \tilde{+} \underset{\sim}{T}^E_{ijs} \tilde{+} \ldots \tilde{+} \underset{\sim}{T}^E_{ijr}) / \eta_{max}. \quad (6)$$

Например, при $i=j=3$ выражение (6), для определения $\underset{\sim}{P}_{33} = \underset{\sim}{P}_{SPKOP}$, будет иметь следующий вид $\underset{\sim}{P}_{33} = (\sum_{s=1}^{5} \underset{\sim}{T}^E_{33s}) / \eta_{max} = (\underset{\sim}{T}^E_{331} \tilde{+} \underset{\sim}{T}^E_{332} \tilde{+} \underset{\sim}{T}^E_{333} \tilde{+} \underset{\sim}{T}^E_{334} \tilde{+} \underset{\sim}{T}^E_{335}) / \eta_{max} = (\underset{\sim}{T}^E_{SPKOP1} \tilde{+} \underset{\sim}{T}^E_{SPKOP2} \tilde{+} \underset{\sim}{T}^E_{SPKOP3} \tilde{+} \underset{\sim}{T}^E_{SPKOP4} \tilde{+} \underset{\sim}{T}^E_{SPKOP5}) / \eta_{max}$.

Поскольку все носители НЧ $\underset{\sim}{M}^E_{36}$ и $\underset{\sim}{B}^E_{36}$ (см. пример этапа 2) имеют нулевые значения, то согласно выражения (6) посредством метода ЛАЛМ [9] реализация вычислений производится следующим образом $\underset{\sim}{P}_{SPKOP} = (\underset{\sim}{T}^E_{SPKOP2} \tilde{+} \underset{\sim}{T}^E_{SPKOP3} \tilde{+} \underset{\sim}{T}^E_{SPKOP4}) / \eta_{max} = (\underset{\sim}{M}^E_{33} \tilde{+} \underset{\sim}{C}^E_{33} \tilde{+} \underset{\sim}{B}^E_{33}) / 60 =$ *({0/0,048; 0,67/0,048; 1/0,378; 0,33/1,5; 0/3}*

$\tilde{+}$ {0/0,336; 0,25/2,646; 1/10,5; 0,5/21; 0/42} $\tilde{+}$ {0/0,756; 0,5/3; 1/6; 0,75/12; 0/12})/60=({0/0,384; 0/2,694; 0/10,548; 0/21,048; 0/42,048; 0/0,384; 0,25/2,694; 0,67/10,548; 0,5/21,048; 0,67/42,048; 0/0,714; 0,25/3,024; 1/10,878; 0,5/21,378; 0/42,378; 0/1,836; 0,25/4,146; 0,33/12; 0,33/22,5; 0/43,5; 0/3,336; 0/5,646; 0/13,5; 0/24; 0/45} $\tilde{+}$ {0/0,756; 0,5/3; 1/6; 0,75/12; 0/12})/60=({0/2,694; 0,25/2,694; 1/10,878; 0,67/42,048; 0/42,048} $\tilde{+}$ {0/0,756; 0,5/3; 1/6; 0,75/12; 0/12})/60=({0/3,45; 0/5,694; 0/8,694; 0/14, 694; 0/14,694; 0/3,45; 0,25/5,694; 0,25/8,694; 0,25/14, 694; 0/14,694; 0/11,636; 0,5/13,878; 1/16,878; 0,75/22,878; 0/22,878; 0/42,804; 0,5/45,048; 0,67/48,048; 0,67/54,048; 0/54,048; 0/42,804; 0/45,048; 0/48,048; 0/54,048; 0/54,048})/60={0/5,694; 0,25/5,694; 1/16,878; 0,67/54,048; 0/54,048}/60=**{0/0,095; 0,25/0,095; 1/0,28; 0,67/0,9; 0/0,9}**.

По аналогии с $\tilde{P}_{SPKOП}$ при $i=3$, $j=6$ с учетом нулевых носителей в $\tilde{M}^{E}_{36}$ (см. пример этапа 2) для $\tilde{P}_{36} = \tilde{P}_{SPKПOA}$ получим $\tilde{P}_{SPKПOA}$ =($\tilde{T}^{E}_{SPKПOA2} \tilde{+} \tilde{T}^{E}_{SPKПOA3}) / \eta_{max}$ =($\tilde{C}^{E}_{36} \tilde{+} \tilde{Б}^{E}_{36}$) / 60 ={0/0,6; 0/4,92; 0/48,12; 0/48,12; 0/0,6; 0,25/4,92; 0,25/48,12; 0/48,12; 0/1,68; 0,67/6; 1/49,2; 0/49,2; 0/12,48; 0,5/16,8; 0,5/60; 0/60; 0/12,48; 0/16,8; 0/60; 0/60})/60={0/4,92; 0,25/4,92; 0,67/6; 1/49,2; 0,5/60; 0/60}/60=**{0/0,082; 0,25/0,082; 0,67/0,1; 1/0,82; 0,5/1; 0/1}**.

В результате выполняемых вычислений, образуются фаззифицированные значения текущих параметров $\tilde{P}_{SPKOП}$ и $\tilde{P}_{SPKПOA}$, графическая интерпретация которых относительно лингвистических эталонов $\mathbf{T^{e}_{33}} = \mathbf{T^{e}_{SPKOП}}$ [6] и $\mathbf{T^{E}_{36}} = \mathbf{T^{e}_{SPKПOA}}$ [7] отображена на рис. 1.

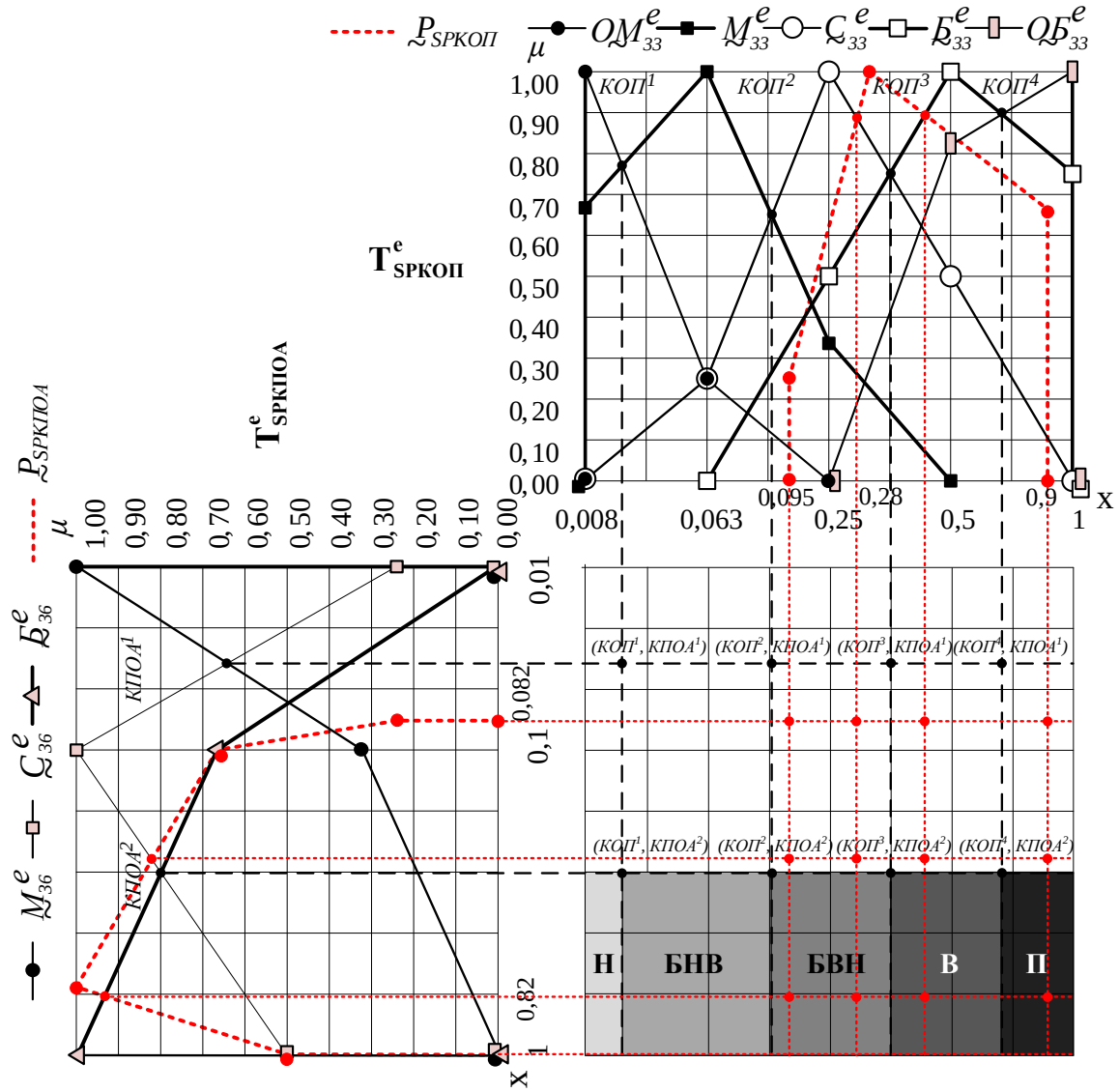

Рис. 1. Графическая интерпретация идентификаторов (образов) атакующих действий (отображаемых двумерными опорными областями Н, БНВ, ББН, В, П) и фаззифицированных значений текущих параметров $\tilde{P}_{SPKOП}$, $\tilde{P}_{SPKПOA}$ относительно лингвистических эталонов $\mathbf{T^{e}_{SPKOП}}$, $\mathbf{T^{e}_{SPKПOA}}$ соответственно

Также на рисунке построены нечеткие опорные двумерные области, характеризующие возможные уровни аномального состояния относительно лингвистических эталонов $\mathbf{T^e_{SPKOП}}$ и $\mathbf{T^e_{SPKПОА}}$ [6, 7] и обозначаются одним из текстовых значений – Н, БНВ, ББН, В, П [3, 8]. С помощью этих эталонов осуществляется поиск нечетких термов $\{T^e_{SPKOП1}, T^e_{SPKOП2}, T^e_{SPKOП3}, T^e_{SPKOП4}, T^e_{SPKOП5}\}$ и $\{T^e_{SPKПОА1}, T^e_{SPKПОА2}, T^e_{SPKПОА3}\}$, которые наиболее близки к соответствующим значениям текущих параметров $P_{SPKOП}$ и $P_{SPKПОА}$, а также определяется опорная двумерная область, отображающая текущий уровень аномального состояния. Дальнейшая формализация процесса такого поиска даст возможность автоматизировать процесс выявления атакующих действий, идентификатором (образом) которых фактически и будут выступать сформированные опорные области (см. рис. 1). Формализацию отдельных процедур поиска можно осуществить, например, посредством подмножеств эвристических правил $\mathbf{ER_3=ER_{SP}}$ [3, 8], которым соответствуют следующие наборы решающих правил, направленных на выявление спуфинга: $\boldsymbol{ER_3}$ $\{ER_{31} = (P_{SPKПОА} \cong Б^e_{36} \wedge P_{SPKOП} \cong ОМ^e_{33}) \rightarrow Н$, $ER_{32} = (P_{SPKПОА} \cong Б^e_{36} \wedge P_{SPKOП} \cong М^e_{33}) \rightarrow БНВ$, $ER_{33} = (P_{SPKПОА} \cong Б^e_{36} \wedge P_{SPKOП} \cong С^e_{33}) \rightarrow ББН$, $ER_{33} = (P_{SPKПОА} \cong Б^e_{36} \wedge P_{SPKOП} \cong Б^e_{33}) \rightarrow В$, $ER_{33} = (P_{SPKПОА} \cong Б^e_{36} \wedge P_{SPKOП} \cong ОБ^e_{33}) \rightarrow П\}$.

Выводы

Предложенный в работе МФПЛЭ, за счет преобразования введенных множеств сенсоров, счетчиков сенсоров и поправочных эталонов, а также использования множеств лингвистических эталонов и соответствующих подмножеств интервалов для формирования частот встречаемости значений физических параметров в заданные моменты наступления ожидаемого события, позволяет фаззифицировать текущие значения параметров для последующего выявления аномального состояния в компьютерных системах.

Следует также отметить, что имея обобщенные описания процесса фаззификации текущих параметров и построения лингвистических эталонов, можно формализовать процесс поиска эталонного значения наиболее близкого к текущему параметру и таким образом повысить эффективность решения задач определения уровня аномального состояния в компьютерных системах.

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. 16. — С. 387-393.

[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] 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.

[6] Корченко А.А. Метод формирования лингвистических эталонов для систем выявления вторжений / А.А. Корченко // Захист інформації. — Т. 16, №1. — 2014. — С. 5-12.

[7] 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.

[8] 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.

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

УДК 004.056.53 (045)

Корченко А. Метод фазифікації параметрів на лінгвістичних еталонах для систем виявлення кібератак

Анотація. *Однією з базових задач в області інформаційної безпеки є створення систем захисту мережевих і системних ресурсів, заснованих на аномальному принципі. Для побудови та розширення функціональності такого роду систем використовується метод виявлення аномалій, породжених кібератаками в інформаційних системах. У цьому методі процес фазифікації параметрів практично не формалізований, що знижує ефективність його використання. З цією метою пропонується метод, який базується на лінгвістичних еталонах, математичних моделях, методах нечіткої логіки та реалізується за допомогою трьох основних етапів: формування частот появи параметрів; формування поправкових еталонів; формування нечітких параметрів. За допомогою цих етапів здійснюється фазифікація поточних значень*

величин при вирішенні задач виявлення кібератак в комп'ютерних системах, що підвищить ефективність побудови відповідних систем виявлення вторгнень.
Ключові слова: *кібератаки, аномалії, нечіткі еталони, лінгвістичні еталони, метод фазифікації параметрів, фазифікація параметрів, системи виявлення вторгнень, системи виявлення аномалій, системи виявлення атак, виявлення аномалій в комп'ютерних мережах.*

Korchenko A. Method of parameter fuzzification based on linguistic standards for cyber attacks detection
Abstract. *One of the basic tasks related to the field of information security is the development of network and system resources protection systems based on the abnormal principle. To develop and extend the functionality of such systems the method of anomaly detection caused by cyber attacks in the information systems is used. In this method the parameters fuzzification process is not formalized, that reduces the efficiency of its use. With this objective the method which is based on linguistic standards, mathematical models, methods of indistinct logic is offered and is realized by means of three basic stages: occurrence and parameters of frequency formation; the formation of correction standards; the development of fuzzy parameters. Through these stages it is carried out the fuzzification of current values at the decision of problems of cyber attacks detection in computer systems that will increase the efficiency of construction of intrusion detection systems.*
Key words: *cyber attacks, anomalies, fuzzy standards, linguistic standards, method of parameter fuzzification, intrusion detection systems, anomaly detection, attack detection, anomaly detection in computer networks.*

Отримано *3 березня 2014 року*, затверджено редколегією *19 березня 2014 року*