УДК 004.056.53(045) **Луцкий М.Г., Гавриленко А.В., Корченко А.А., Охрименко А.А.**

МОДЕЛИ ЭТАЛОНОВ ЛИНГВИСТИЧЕСКИХ ПЕРЕМЕННЫХ ДЛЯ СИСТЕМ ВЫЯВЛЕНИЯ АТАК

Предложена модель эталонов лингвистических переменных, которая ориентирована на построение систем выявления атак, основанных на идентификации аномального состояния в информационной системе. Для выявления DDoS-атак и спуфинга используются параметры: количество одновременных подключений к серверу, скорость обработки запросов от клиентов, задержка между запросами от одного пользователя, количество пакетов с одинаковым адресом отправителя и получателя. На основе данных проведенного эксперимента построены модели эталонов параметров с использованием базовых терм-множеств и нечетких чисел.

Ключевые слова: атака, аномалия, идентификация аномалий, системы выявления атак, лингвистические переменные, эталоны параметров, лингвистические модели, нечеткие числа.

В стремительно развивающейся информационной среде появляются новые виды угроз ее ресурсам. В этой связи существует потребность в системах безопасности, позволяющих анализировать, контролировать, прогнозировать и блокировать новые виды атак в информационной системе (ИС). Для этого необходимы средства, дающие возможность выявить нападение по характерным признакам.

Несанкционированные воздействия на ресурсы ИС оказывают влияние на среду их окружения и порождают определенные аномалии. Для их идентификации можно использовать логико-лингвистический подход [1] и базовую моделью параметров (БМП) [2], которые могут стать основой построения систем выявления атак. Согласно БМП следует определить набор величин, необходимый для обнаружения подозрительной активности в сетевом трафике. Например, для обнаружения процесса сканирования портов в работах [1, 3, 4] используются лингвистические переменные (ЛП) “КОЛИЧЕСТВО ВИРТУАЛЬНЫХ КАНАЛОВ” (**КВК**) и “ВОЗРАСТ ВИРТУАЛЬНОГО КАНАЛА” (**ВВК**), соответственно определяемые кортежами <КВК, $Т_{КВК}$, $Х_{КВК}$> и <ВВК, $Т_{ВВК}$, $Х_{ВВК}$>. Виртуальный канал (ВК) создается при получении приемником IP-пакета и существует определенное время. Признаком рождения новых ВК, служит прием IP-пакета на порт, для которого такой канал отсутствовал. Максимальное число ВК определяется значением $max_{КВК}$ и часто определяется количеством доступных портов, например, 65536. Параметр “время жизни” (ВЖ) отражает остаток времени существования ВК, а в момент его создания $ВЖ:=ВЖ_0$, (1 мин$\le ВЖ_0 \le$10 мин). Канал прекращает существование при $ВЖ=0$, а при очередном IP-пакете $ВЖ:=ВЖ+\Delta ВЖ$ (например, $\Delta ВЖ$=100 мс). Очевидно, что при интенсивном трафике для ВК ВЖ увеличивается, и он долго существует, а при остановке обмена через время $ВЖ_Т$ ($ВЖ_Т$ – текущее значение ВЖ) канал удаляется, т.е. чем интенсивнее трафик, тем живучее канал. На основе свойств ВК и соответствующих ему ЛП формируются эталонные параметры для выявления сканирования портов.

Процесс идентификации аномалий, порожденных другими возможными атаками на ресурсы информационных систем (ИС) также требует определения необходимых параметров и их свойств. В связи с этим, целью данной работы является построение моделей эталонов параметров, позволяющих расширить возможности соответствующих систем защиты за счет обнаружения других видов атак в нечетко определенной, слабоформализированной среде. Например, основываясь на [6, 7, 9, 10] для выявления DDoS-атак на сервер и спуфинга наиболее целесообразно использовать следующие параметры: количество одновременных подключений (КОП) к серверу; скорость обработки запросов (СОЗ) от клиентов; задержка между запросами (ЗМЗ) от одного пользователя, количество пакетов с одинаковым адресом отправителя и получателя (КПОА). Как показывает практика для эффективного проведения DDoS необходимо привлечение большого количества источников, участвующих в нападении

на жертву. Следовательно, параметр КОП при увеличении количества подключений к серверу может использоваться в качестве одного из признаков начала атаки. Максимальное число подключений, которое может поддерживать сервер, зависит от его аппаратных и программных возможностей и характеризуется параметром $max_{КОП}$, значение которого будет отличаться для разных серверов.

Возможность противостоять нападениям во многом зависит от такого важного сетевого параметра в работе серверов, как СОЗ, характеризующий возможное количество запросов, обрабатываемых за единицу времени (обычно за секунду). При большом количестве запросов, которые генерируют участники DDoS-атаки, сервер полностью или частично перестает реагировать на запросы легитимных пользователей, то есть не справляется с нагрузкой. Максимальная скорость обработки запросов определяется на практике с помощью стресс-тестов для конкретного сервера в конкретной среде окружения и задается параметром $max_{СОЗ}$.

Параметр ЗМЗ характеризует время между последовательными запросами от одного подключенного к серверу клиента. На некоторых серверах для предотвращения атак этот параметр устанавливается вручную (например, 1 запрос за 1 секунду от пользователя). Уменьшение задержки между запросами может свидетельствовать о начале DDoS-атаки, целью которой является отправка как можно большего количества запросов, которые выведут сервер из работоспособного состояния. Значение ЗМЗ определяется величиной $max_{СОЗ}$, которая зависит от программного обеспечения (ПО) и назначения сервера.

Для получения конкретных числовых параметров проводится эксперимент на реальном работающем Web-сервере. В качестве примера тестируемого сервера был выбран компьютер (процессор Intel(R) Celeron(R) CPU 2.80GHz с частотой шины 133 МГц; оперативная память 2 Гб DDR2 400 МГц; сетевое подключение – 100 Мбит/с; операционная система – 32-битная Debian GNU/Linux 6.0.3 (squeeze)) со следующим списком установленного основного ПО: Apache 2.2.16, BIND DNS сервер 9.7.1, Exim 4.72, lighttpd 1.4.28, MySQL 5.1.49, OpenSSH 5.5p1, PHP 5.3.2, Tomcat 6.0.28, Iptables.

Максимальное значение параметра КОП определяется в настройках Web-сервера как *MaxClients* по адресу */etc/apache2/apache2.conf*. Система сконфигурирована таким образом, чтобы поддерживать одновременно максимум 1024 подключения. Согласно статистике, собраной с помощью утилиты *Netstat,* для данного сервера среднее количество таких подключений не превышало 100.

Значения параметра СОЗ были получены по результатам стресс-теста, осуществляемого с помощью утилиты Apache HTTP server benchmarking tool [5, 11], которая является одним из самых распространенных средств для оценки производительности и входит в базовый пакет программ Apache. Измерения проводились при большом количестве запросов, которые показали, что данный Web-сервер может обработать до 1200 запросов в секунду в локальной сети, и около 100 (см. рис. 1) полученных из сети Internet. В нормальном режиме работы сервер за одну секунду обслуживает около 34 Internet-запросов.

Поскольку существует множество различных запросов (как пользовательских так и служебных), то определение величины ЗМЗ от одного пользователя имеет определенную специфику, причем в сетевом трафике они отличаются по частоте встречаемости и времени обработки сервером. Следовательно методика измерения должна включать только те запросы, которые являются наиболее затратными для сервера с точки зрения его производительности. В частности, ICMP-запросы проходят фильтрацию с помощью установленных политик безопасности на межсетевом экране Iptables. Для измерения интервалов времени между наиболее частыми для Web-серверов запросов GET и POST был написан php-скрипт, который анализирует обращения к серверу и вычисляет время между двумя последовательными запросами GET или POST от пользователя, усредненное значение $max_{ЗМЗ}$ для которых составило приблизительно 200 мс и 1 с соответственно.

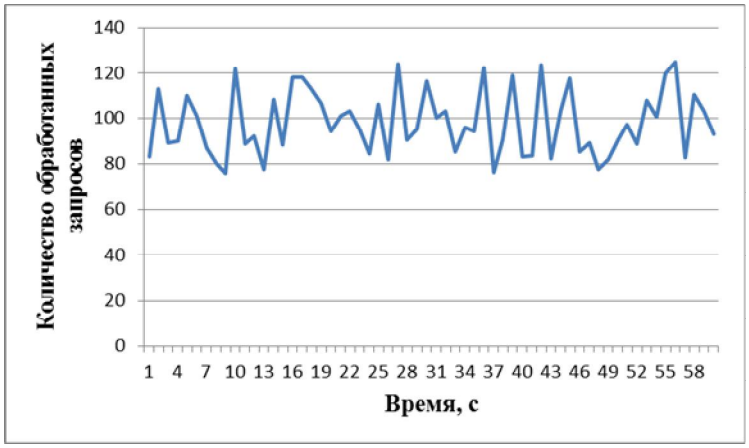

Рис.1. Результаты стресс-теста обработки Internet-запросов за 60 сек

Для выявления спуфинга направленного на вызов DoS- или провокация DDoS-аткаки используем признаки, характеризующиеся подменой адресов в заголовке пакетов. Поэтому для выявления такой атаки целесообразно использовать параметр КПОА. Здесь, в частности рассматривается вид спуфинга, при котором неавторизированная сторона генерирует большое количество пакетов, в заголовках которых в качестве адреса отправителя и получателя указан адрес сервера, который отвечая на полученные запросы атакует сам себя. Возникновение большого количества пакетов с одинаковым адресом получателя и отправителя в сетевом траффике может свидетельствовать о начале DDoS-атаки.

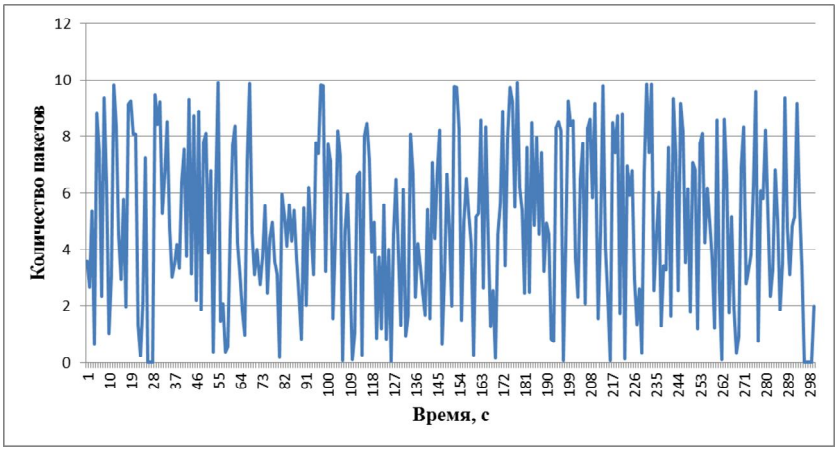

Рис. 2. Значение КПОА при работе сервера на протяжении 5 минут

Значение параметра КПОА определялось на основе данных, полученных при обработке логов межсетевого экрана Iptables. Методика измерений подразумевает подсчет количества пакетов в заголовках которых указаны одинаковые адреса и порты получателя и отправителя (SRC и DST) за единицу времени. Согласно подсчету (см. рис. 2), при нормальной работе сервера количество пакетов с одинаковым адресом получателя и отправителя не превышает 10 за секунду. Следовательно, превышение этого значения в определенное число раз может быть признаком спуффинг-атаки на сервер.

Одними из ключевых величин в БМП являются эталоны параметров, которые строятся для ЛП и необходимы при формировании логических правил, используемых при выявлении нападений. В этой связи, построим лингвистические модели эталонов параметров для ЛП **КОП, СОЗ, ЗМЗ** и **КПОА** с кортежами $<КОП, T_{КОП}, U_{КОП}>$, $<СОЗ, T_{СОЗ}, U_{СОЗ}>$, $<ЗМЗ, T_{ЗМЗ}, U_{ЗМЗ}>$ и $<КПОА, T_{КПОА}, U_{КПОА}>$ соответственно.

С учетом проведенного эксперимента модель эталонов для $<КОП, T_{КОП}, U_{КОП}>$ построим на основе базового терм-множества с пятью нечеткими термами: $T_{КОП}=\bigcup_{i=1}^{5} T^{i}_{КОП}$ ={*“ОЧЕНЬ МАЛОЕ” (ОМ), “МАЛОЕ” (М), “СРЕДНЕЕ” (С), “БОЛЬШОЕ” (Б), “ОЧЕНЬ БОЛЬШОЕ” (ОБ)*}, которые могут быть отображены на универсальное множество $U_{КОП} \in \{0, max_{КОП}\}$.

Воспользуясь экспертными оценками, сделанными на базе данных табл. 1, сформируем функции принадлежности (ФП) для $T_{КОП}$, основываясь на методе лингвистических термов с использованием статистических данных МЛТС [1].

Данные для $T_{КОП}$ Таблица 1

Значения ЛП	Интервал				
	N1	N2	N3	N4	N5
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

Практика показывает, что наиболее целесообразно определить $max_{КОП}=1024$ (значение *MaxClients* в настройках сервера), а *N1, N2, N3, N4, N5* определить соответственно интервалами [0; 8], [9; 64], [65; 256], [257; 512], [513; 1024]. Для последующего получения эталонов сформируем матрицу подсказок по формуле $\|k_j\| = \left\| \bigcup_{j=1}^{5} \sum_{i=1}^{5} b_{ij} \right\| = \|6,5,7,11,9\|$, где b_{ij} – элементы эмпирических данных (см. табл. 1), которые преобразовываются в матрицу по выражению:

$$c_{ij} = b_{ij} km / k_j, \quad (1)$$

где $(i, j = \overline{1,5})$, а $km = \bigvee_{j=1}^{5} k_j = 11$, и

$$\|c_{ij}\| = \begin{Vmatrix} 7,33 & 1,83 & 0 & 0 & 0 \\ 4,4 & 6,6 & 2,2 & 0 & 0 \\ 0 & 1,57 & 6,29 & 3,14 & 0 \\ 0 & 0 & 2 & 4 & 3 \\ 0 & 0 & 0 & 6,11 & 7,33 \end{Vmatrix}.$$

Далее вычисляется матрица ФП по выражению:

$$\mu_{ij} = c_{ij} / cm_i, \quad (2)$$

где $(i, j = \overline{1,5})$, а $cm_i = \bigcup_{j=1}^{5} \bigvee_{i=1}^{5} c_{ij} = \{7,33;\ 6,6;\ 6,29;\ 4;\ 7,33\}$. Полученные значения имеют следующий вид:

$$\|\mu_{ij}\| = \begin{Vmatrix} 1 & 0,25 & 0 & 0 & 0 \\ 0,67 & 1 & 0,33 & 0 & 0 \\ 0 & 0,25 & 1 & 0,5 & 0 \\ 0 & 0 & 0,5 & 1 & 0,75 \\ 0 & 0 & 0 & 0,83 & 1 \end{Vmatrix}.$$

Для $\bigcup_{i=1}^{5} \mu_{ij}$ соответственно находим оценочные отношения $\bigcup_{i=1}^{5} \Delta B_i / B = \{0,008;\ 0,063;\ 0,25;\ 0,5;\ 1\}$ ($\Delta B/B$ – отклонение параметра $\Delta B_{КОП} \in [0,\ B_{КОП}]$, а $B_{КОП}$ – максимально возможное значение, которое характеризует текущие измерения) и получаем промежуточные нечеткие числа (НЧ): $\underset{\sim}{ОМ}$ ={1/0,008; 0,25/0,063; 0/0,25; 0/0,5; 0/1}; $\underset{\sim}{М}$ ={0,67/0,008; 1/0,063; 0,33/0,25; 0/0,5; 0/1}; $\underset{\sim}{С}$ ={0/0,008; 0,25/0,063; 1/0,25; 0,5 /0,5; 0/1}; $\underset{\sim}{Б}$ ={0/0,008; 0/0,063; 0,5/0,25; 1/0,5; 0,75/1}; $\underset{\sim}{ОБ}$ ={0/0,008; 0/0,063; 0/0,25; 0,83/0,5; 1/1}.

Для формирования лингвистических эталонов необходимо чтобы для $\forall T^{i}_{КОП}$ было справедливо отношение порядка, например, при i=1, $\forall x_{ОМ}$: $x_{ОМ_k} < x_{ОМ_{k+1}}$. Далее полученные $T_{КВК}$ для НЧ $\underset{\sim}{X}$={μ_1/x_1; … μ_i/x_i; … μ_n/x_n} представляются в приведенной форме [1] $T^{e}_{КОП} = \bigcup_{i=1}^{5} T^{ei}_{КОП} = \{\underset{\sim}{ОМ}^{e},\ \underset{\sim}{М}^{e},\ \underset{\sim}{С}^{e},\ \underset{\sim}{Б}^{e},\ \underset{\sim}{ОБ}^{e}\}$, где $\underset{\sim}{ОМ}^{e}$ ={0/0,008; 1/0,008; 0,25/0,063; 0/0,25};

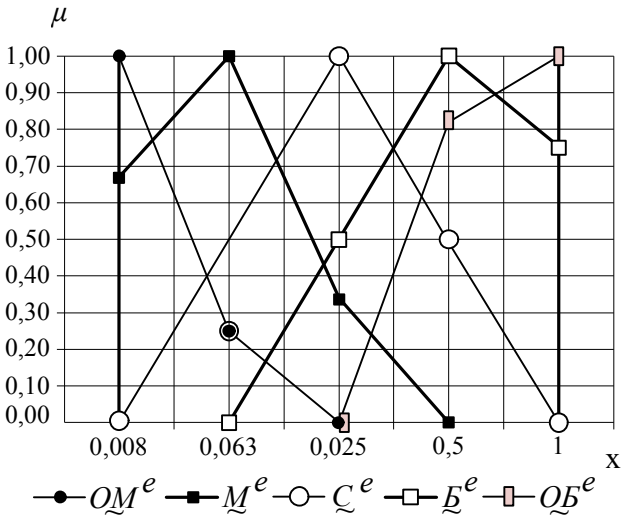

Рис. 3. Лингвистические эталоны НЧ для **КОП**

$\underset{\sim}{M}^e$ ={0/0,008; 0,67/0,008; 1/0,063; 0,33/0,25; 0/0,5}; $\underset{\sim}{C}^e$ ={0/0,008; 0,25/0,063; 1/0,25; 0,5/0,5; 0/1}; $\underset{\sim}{Б}^e$ ={0/0,063; 0,5/0,25; 1/0,5; 0,75/1; 0/1}; $\underset{\sim}{ОБ}^e$ ={0/0,25; 0,83/0,5; 1/1; 0/1}.

Полученные значения и будут использоваться в качестве эталонных для **КОП**, графическое изображение которых представлено на рис. 3.

С учетом проведенного эксперимента модель эталонов для <*СО3, T_{CO3}, U_{CO3}*> построим на основе базового терм-множества с тремя нечеткими термами: $T_{CO3}=\bigcup_{i=1}^{3} T^i_{CO3}$ ={*“НИЗКАЯ” (Н), “СРЕДНЯЯ” (С), “ВЫСОКАЯ” (В)*}, которые могут быть отображены на универсальное множество $U_{CO3}\in\{0, max_{CO3}\}$.

Данные для T_{CO3} Таблица 2

Значения ЛП	Интервал		
	N1	N2	N3
Н	3	1	0
С	1	2	1
В	0	1	4

На основе экспертных данных в табл. 2 сформируем ФП для интервалов *N1, N2, N3*, принимающих соответственно значения [0; 5], [6; 25], [26; 100]. Согласно эксперименту (см. рис. 1) определим $max_{CO3}=100$, отражающее усредненное значение количества пакетов с сети Internet, полученное с помощью стресс-теста.

Формируем матрицу подсказок по формуле $\|k_j\|=\left\|\bigcup_{j=1}^{3}\sum_{i=1}^{3} b_{ij}\right\|=\|4,4,5\|$, где b_{ij} – элементы эмпирических данных (см. табл. 2), которые преобразовываются в матрицу по выражению (1) при $(i,j=\overline{1,3})$, где $km=\bigvee_{j=1}^{3} k_j$ =5, а

$$\|c_{ij}\|=\begin{Vmatrix} 3,75 & 1,25 & 0 \\ 1,25 & 2,5 & 1 \\ 0 & 1,25 & 4 \end{Vmatrix}.$$

Далее вычисляем ФП по выражению (2) при $(i,j=\overline{1,3})$, где $cm_i=\bigcup_{j=1}^{3}\bigvee_{i=1}^{3} c_{ij}$ ={*3,75; 2,5; 4*}. Вычисленные значения ФП будут следующие:

$$\|\mu_{ij}\|=\begin{Vmatrix} 1 & 0,33 & 0 \\ 0,5 & 0,9 & 0,4 \\ 0 & 0,31 & 1 \end{Vmatrix}.$$

Для $\bigcup_{i=1}^{3}\mu_{ij}$ соответственно находим оценочные отношения $\bigcup_{i=1}^{3}\Delta B_i / B$ ={*0,05; 0,25; 1*} (*ΔB/B* – отклонение параметра $\Delta B_{CO3}\in[0, B_{CO3}]$, а B_{CO3} – максимально возможное значение, которое характеризует текущие измерения) и получаем НЧ: $\underset{\sim}{H}$ ={*1/0,05; 0,33/0,25; 0/1*}; $\underset{\sim}{C}$ ={*0,5/0,05; 0,9/0,25; 0,4/1*}; $\underset{\sim}{B}$ ={*0/0,05; 0,31/0,25; 1/1*}.

Учитывая, что для $\forall T_{СОЗ}^{i}$ справедливо отношение порядка, например, при i=1, $\forall x_M$: $x_{H_k} < x_{H_{k+1}}$. Полученные $T_{СОЗ}$ для НЧ $\underset{\sim}{X}=\{\mu_1/x_1;\ \dots\ \mu_i/x_i;\ \dots\ \mu_n/x_n\}$ представляются в приведенной форме [1] $T_{СОЗ}^{e}=\bigcup_{i=1}^{3} T_{СОЗ}^{ei}=\{\underset{\sim}{H}^{e},\ \underset{\sim}{C}^{e},\ \underset{\sim}{B}^{e}\}$, где $\underset{\sim}{H}^{e}=\{0/0,05;\ 1/0,05;\ 0,33/0,25;\ 0/1\}$;

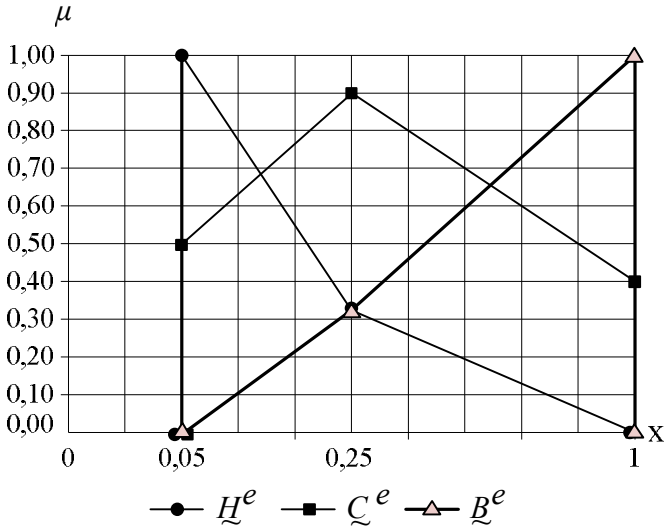

Рис. 4 Эталонные НЧ для **СОЗ**

$\underset{\sim}{C}^{e}=\{0/0,05;\ 0,5/0,05;\ 0,9/0,25;\ 0,4/1;\ 0/1\}$;

$\underset{\sim}{B}^{e}=\{0/0,05;\ 0,31/0,25;\ 1/1;\ 0/1\}$.

Полученные значения и будут использоваться в качестве эталонных для **СОЗ**, графическое изображение которых представлено на рис. 4.

По аналогии с СОЗ проведем вычисления для *<ЗМЗ, $T_{ЗМЗ}$, $U_{ЗМЗ}$>* с использованием терм-множества на три нечетких терма: $T_{ЗМЗ}=\bigcup_{i=1}^{3} T_{ЗМЗ}^{i}=\{$*"МАЛАЯ" (М), "СРЕДНЯЯ" (С), "ВЫСОКАЯ" (В)*$\}$, которые отображаются на универсальное множество $U_{ЗМЗ}\in\{0,\ max_{ЗМЗ}\}$.

Данные для $T_{ЗМЗ}$ Таблица 3

Значения ЛП	Интервал		
	N1	N2	N3
М	3	1	0
С	1	3	2
В	0	2	5

По табл. 3 для *N1, N2, N3* соответственно зададим значения [0; 10], [11; 100], [101; 1000]. Согласно эксперименту (см. рис. 1) определим значение $max_{ЗМЗ}=1000$ мс на основе полученных данных по времени обработки запросов GET и POST. Формируем матрицу подсказок по формуле $\|k_j\|=\left\|\bigcup_{j=1}^{3}\sum_{i=1}^{3} b_{ij}\right\|=\|4,6,7\|$, где b_{ij} – элементы эмпирических данных (см. табл. 3), которые преобразовываются в матрицу по выражению (1) при $(i,j=\overline{1,3})$, где $km=\bigvee_{j=1}^{3} k_j=7$, а

$$\|c_{ij}\|=\begin{Vmatrix} 5,25 & 1,75 & 0 \\ 1,17 & 3,5 & 2,33 \\ 0 & 2 & 5 \end{Vmatrix}.$$

Далее вычисляем ФП по выражению (2) при $(i,j=\overline{1,3})$, где $cm_i=\bigcup_{j=1}^{3}\bigvee_{i=1}^{3} c_{ij}=\{5,25;\ 3,5;\ 5\}$. Вычисленные значения ФП будут следующие:

$$\|\mu_{ij}\|=\begin{Vmatrix} 1 & 0,33 & 0 \\ 0,33 & 1 & 0,67 \\ 0 & 0,4 & 1 \end{Vmatrix}.$$

Для $\bigcup_{i=1}^{3}\mu_{ij}$ соответственно находим оценочные отношения $\bigcup_{i=1}^{3}\Delta B_i / B=\{0,01;\ 0,1;\ 1\}$ ($\Delta B/B$ – отклонение параметра $\Delta B_{ЗМЗ}\in[0,\ B_{ЗМЗ}]$, а $B_{ЗМЗ}$ – максимально возможное значение, которое характеризует текущие измерения) и получаем НЧ: $\underset{\sim}{M}=\{1/0,01;\ 0,33/0,1;\ 0/1\}$; $\underset{\sim}{C}=\{0,33/0,01;\ 1/0,1;\ 0,67/1\}$; $\underset{\sim}{B}=\{0/0,01;\ 0,4/0,1;\ 1/1\}$.

При формировании эталонов для $\forall T^i_{ЗМЗ}$ также справедливо отношение порядка, например, при i=1, $\forall x_M$: $x_{M_k} < x_{M_{k+1}}$. Далее $T_{ЗМЗ}$ для НЧ $\underset{\sim}{X}=\{\mu_1/x_1;\ \dots\ \mu_i/x_i;\ \dots\ \mu_n/x_n\}$ представляются в приведенной форме [1] $T^e_{ЗМЗ}=\bigcup_{i=1}^{3} T^{ei}_{ЗМЗ}=\{\underset{\sim}{M}^e,\ \underset{\sim}{C}^e,\ \underset{\sim}{B}^e\}$, где $\underset{\sim}{M}^e=\{0/0{,}01;\ 1/0{,}01;\ 0{,}33/0{,}1;\ 0/1\}$; $\underset{\sim}{C}^e=\{0/0{,}01;\ 0{,}33/0{,}01;\ 1/0{,}1;\ 0{,}67/1;\ 0/1\}$; $\underset{\sim}{B}^e=\{0/0{,}01;\ 0{,}4/0{,}1;\ 1/1;\ 0/1\}$. Эти значения и будут использоваться в качестве эталонных для **ЗМЗ**, графическое изображение которых представлено на рис. 5.

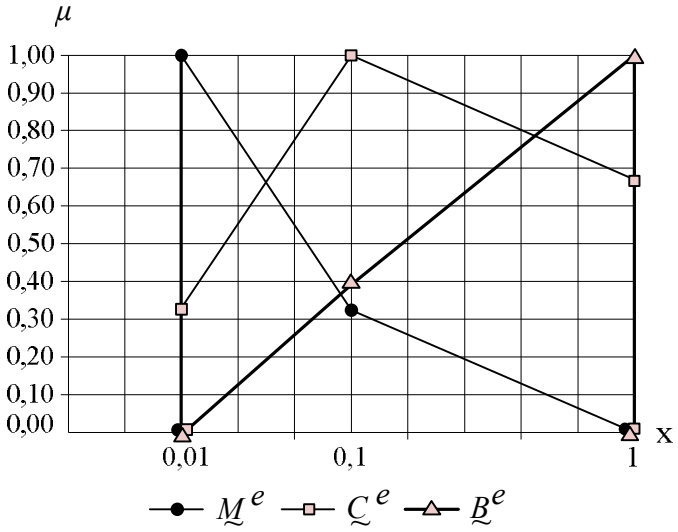

Рис. 5. Эталонные НЧ для **ЗМЗ**

По принципу с ЗМЗ также осуществим вычисления для *<КПОА, $T_{КПОА}$, $U_{КПОА}$>* на основе $T_{КПОА}=\bigcup_{i=1}^{3} T^i_{КПОА}$ = *{“МАЛОЕ” (М), “СРЕДНЕЕ” (С), “БОЛЬШОЕ” (Б)}*, а нечеткие термы могут быть отображены на универсальное множество $U_{КПОА}\in\{0,\ max_{КПОА}\}$.

Данные для $T_{КПОА}$ Таблица 4

Значения ЛП	Интервал		
	N1	N2	N3
М	3	1	0
С	1	4	2
Б	0	2	3

С использованием данных в табл. 4 для интервалов *N1, N2, N3* установим значения [0; 10], [11; 100], [101; 1000]. Согласно эксперименту (см. рис. 5) на основе мониторинга конкретного работающего сервера определим значение $max_{КПОА}=1000$ пакетов (превышение нормального значения количества пакетов в 100 раз).

Формируем матрицу подсказок по формуле $\|k_j\|=\left\|\bigcup_{j=1}^{3}\sum_{i=1}^{3} b_{ij}\right\|=\|4,7,5\|$, где b_{ij} – элементы эмпирических данных (см. табл. 4), которые преобразовываются в матрицу по выражению (1) при $(i,j=\overline{1,3})$, где $km=\bigvee_{j=1}^{3} k_j$ =7, а

$$\|c_{ij}\|=\begin{Vmatrix} 5{,}25 & 1{,}75 & 0 \\ 1 & 4 & 2 \\ 0 & 2{,}8 & 4{,}2 \end{Vmatrix}.$$

Далее вычисляем ФП по выражению (2) при $(i,j=\overline{1,3})$, где $cm_i=\bigcup_{j=1}^{3}\bigvee_{i=1}^{3} c_{ij}=\{5{,}25;\ 4;\ 4{,}2\}$. Вычисленные значения ФП будут следующие:

$$\|\mu_{ij}\|=\begin{Vmatrix} 1 & 0{,}33 & 0 \\ 0{,}25 & 1 & 0{,}5 \\ 0 & 0{,}67 & 1 \end{Vmatrix}.$$

Для $\bigcup_{i=1}^{3}\mu_{ij}$ соответственно находим оценочные отношения $\bigcup_{i=1}^{3}\Delta B_i / B=\{0{,}01;\ 0{,}1;\ 1\}$ ($\Delta B/B$ – отклонение параметра $\Delta B_{КПОА}\in[0,\ B_{КПОА}]$, а $B_{КПОА}$ – максимально возможное значение, которое характеризует текущие измерения) и получаем НЧ: $\underset{\sim}{M}=\{1/0{,}01;\ 0{,}33/0{,}1;\ 0/1\}$; $\underset{\sim}{C}=\{0{,}25/0{,}01;\ 1/0{,}1;\ 0{,}5/1\}$; $\underset{\sim}{Б}=\{0/0{,}01;\ 0{,}67/0{,}1;\ 1/1\}$.

А также, формируя эталоны для $\forall T^{i}_{КПОА}$ справедливо отношение порядка, например, при i=1, $\forall x_M$: $x_{M_k} < x_{M_{k+1}}$. Далее полученные $T_{КПОА}$ для НЧ $\underset{\sim}{X}=\{\mu_1/x_1;\ \dots\ \mu_i/x_i;\ \dots\ \mu_n/x_n\}$ представляются в приведенной форме [1] $T^{e}_{КПОА}=\bigcup_{i=1}^{3} T^{ei}_{КПОА}=\{\underset{\sim}{M}^{e}, \underset{\sim}{C}^{e}, \underset{\sim}{B}^{e}\}$, где $\underset{\sim}{M}^{e}=\{0/0{,}01;$ $1/0{,}01;$ $0{,}33/0{,}1;$ $0/1\};$ $\underset{\sim}{C}^{e}=\{0/0{,}01;$ $0{,}25/0{,}01;$ $1/0{,}1;$ $0{,}5/1;$ $0/1\};$ $\underset{\sim}{Б}^{e}=\{0/0{,}01;$ $0{,}67/0{,}1;$ $1/1;$ $0/1\}$. Полученные значения, как и в предыдущих моделях, будут использоваться в качестве эталонных для **КПОА**, графическое изображение которых представлено на рис. 6.

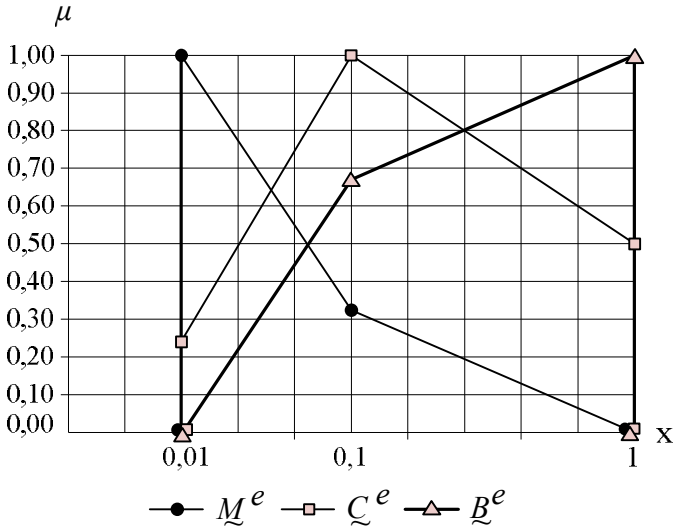

Рис. 6. Эталонные НЧ для **КПОА**

В результате проведенной работы, на основе БМП с использованием данных экспертных оценок, были построены лингвистические модели эталонов параметров ЛП **КОП, СОЗ, ЗМЗ, КПОА**. С учетом экспериментальных данных определены конкретные эталонные НЧ, которые необходимы для формирования логических правил, позволяющих повысить эффективность соответствующих средств безопасности, основанных на идентификации аномального состояния в ИС.

ЛИТЕРАТУРА

1. Корченко А.Г. Построение систем защиты информации на нечетких множествах : Теория и практические решения / А.Г.Корченко. – К. : МК-Пресс, 2006. – 320 с.
2. Стасюк А.И., Корченко А.А. Базовая модель параметров для построения систем выявления атак / А.И. Стасюк, А.А. Корченко // Захист інформації. — 2012. — №2 (55) . — С. 47-51.
3. Корченко А.О. Система виявлення аномалій на основі нечітких моделей / А.О. Корченко, Є.В. Паціра, В.В. Волянська // Сучасні тренажерно-навчальні комплекси та системи : Зб. наук. праць. – Л.: Інституту проблем моделювання в енергетиці НАН України ім. Г.Є. Пухова, 2007. □ Т.2. – С. 56 – 60.
4. Програма захисту інформаційних ресурсів від атакуючих дій в комп'ютерних мережах : Комп'ютерна програма / Васюхін М.І., Гулевець В.Д., Корченко А.О., та інші — К. : Інститут кібернетики ім. В.М. Глушкова НАНУ, 2011. — Свідоцтво про реєстрацію авторського права на твір №37127 від 25.02.2011.
5. [ab : Apache HTTP server benchmarking tool] / Electronic data and programs. — The Apache Software Foundation, 2011. — Mode of access: World Wide Web. — URL: http://httpd.apache.org/docs/2.0/programs/ab.html.
6. Gavrilis D. Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features / Gavrilis D., Dermatas E. // Computer Networks. — 2005. — 48. – P. 235–245.
7. McClure S. Hacking exposed, network security secrets & solutions / McClure S., Scambray J., Kurtz G. — 6th Edition. — McGraw-Hill Osborne Media, 2009. – 720 p.
8. Okhrimenko A. Classification denial of service attacks and modern countermeasure techniques / A. Okhrimenko // Тез. доп. першої міжнар. наук.-пр. конф. мол. вчених «Інфокомунікації – сучасність та майбутнє». – Ч.2. – О.: ОНАЗ, 2011. – С. 87-90.
9. Patrikakis C. Distributed denial of service attacks / Patrikakis C., Masikos M., Zouraraki O. // The Internet Protocol Journal. — 2004. – Vol. 7. — № 4. – P. 13-35.
10. Технический отчет: Угрозы DDoS – риски, устранение и лучшие практические приемы [Электронный ресурс]: World Wide Web. — URL: http://www.cisco.com/web/RU/netsol/ns480/networking_solutions_white_paper0900aecd8032499e.html.
11. [Performance Benchmarks a Webserver : Howto] / [Vivek Gite]. — Electronic data and programs. — [Scottsdale]. [2008]. — Mode of access: World Wide Web. — URL: http://www.cyberciti.biz/tips/howto-performance-benchmarks-a-web-server.html.

Надійшла: 12.06.2012

Рецензент: д.т.н., проф. Філоненко С.Ф.