

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 модель 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 $\langle \text{КВК}, T_{\text{КВК}}, X_{\text{КВК}} \rangle$ и $\langle \text{ВВК}, T_{\text{ВВК}}, X_{\text{ВВК}} \rangle$. 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 $\text{max}_{\text{КВК}}$ и часто определяется количеством доступных портов, например, 65536. Параметр “время жизни” (ВЖ) отражает остаток времени существования ВК, а в момент его создания $VЖ: = VЖ_0$, ($1 \text{ мин} \leq VЖ_0 \leq 10 \text{ мин}$). Канал прекращает существование при $VЖ = 0$, а при очередном IP-пакете $VЖ: = VЖ + \Delta VЖ$ (например, $\Delta VЖ = 100 \text{ мс}$). Очевидно, что при интенсивном трафике для ВК ВЖ увеличивается, и он долго существует, а при остановке обмена через время $VЖ_T$ ($VЖ_T$ – 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, слабоформализованной 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, собранной 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.

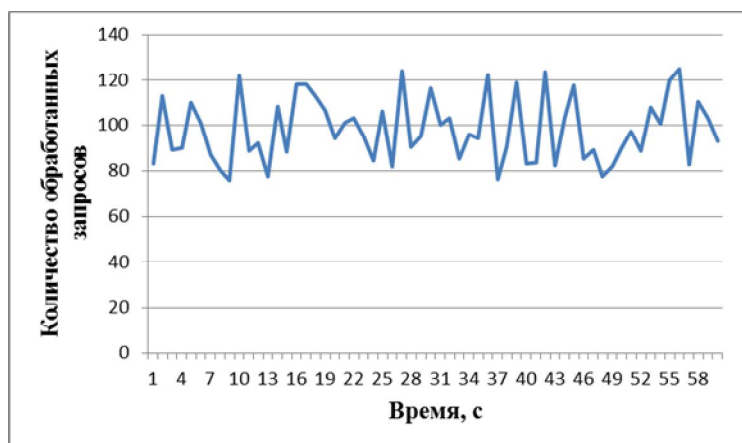


Рис. 1. Результаты стресс-теста обработки Internet-запросов за 60 сек

адрес сервера, который отвечая на полученные запросы атакует сам себя. Возникновение большого количества пакетов с одинаковым адресом получателя и отправителя в сетевом трафике может свидетельствовать о начале DDoS-атаки.

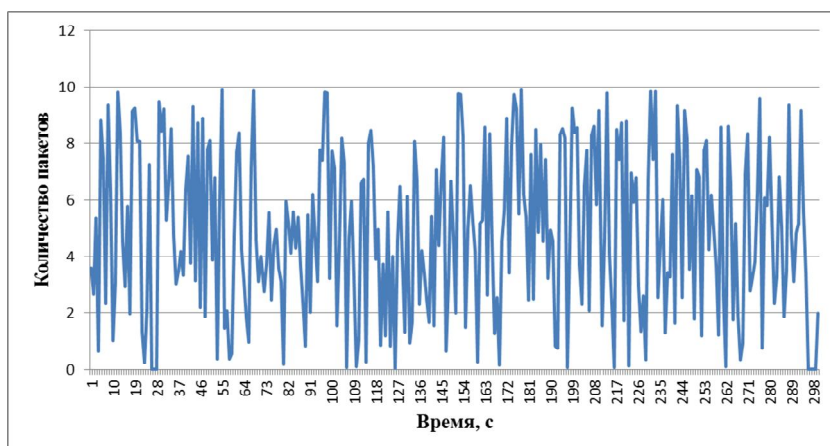


Рис. 2. Значение КПОА при работе сервера на протяжении 5 минут

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 $\langle \text{КОП}, T_{\text{КОП}}, U_{\text{КОП}} \rangle$, $\langle \text{СОЗ}, T_{\text{СОЗ}}, U_{\text{СОЗ}} \rangle$, $\langle \text{ЗМЗ}, T_{\text{ЗМЗ}}, U_{\text{ЗМЗ}} \rangle$ и $\langle \text{КПОА}, T_{\text{КПОА}}, U_{\text{КПОА}} \rangle$ соответственно.

С учетом проведенного эксперимента модель эталонов для $\langle \text{КОП}, T_{\text{КОП}}, U_{\text{КОП}} \rangle$ построим на основе базового терм-множества с пятью нечеткими термами:

$T_{\text{КОП}} = \bigcup_{i=1}^5 T_{\text{КОП}}^i = \{ \text{“ОЧЕНЬ МАЛОЕ” (ОМ), “МАЛОЕ” (М), “СРЕДНЕЕ” (С), “БОЛЬШОЕ” (Б), “ОЧЕНЬ БОЛЬШОЕ” (ОБ)} \}$, которые могут быть отображены на универсальное множество $U_{\text{КОП}} \in \{0, \text{max}_{\text{КОП}}\}$.

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

Для выявления спуффинга направленного на вызов DoS- или провокация DDoS-атаки используем признаки, характеризующиеся подменой адресов в заголовке пакетов. Поэтому для выявления такой атаки целесообразно использовать параметр КПОА. Здесь, в частности рассматривается вид спуффинга, при котором неавторизованная сторона генерирует большое количество пакетов, в заголовках которых в качестве адреса отправителя и получателя указан

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

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:

$$c_{ij} = b_{ij} km / k_j, \tag{1}$$

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:

$$\mu_{ij} = c_{ij} / cm_i, \tag{2}$$

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): $\widetilde{ОМ} = \{1/0,008; 0,25/0,063; 0/0,25; 0/0,5; 0/1\}$; $\widetilde{М} = \{0,67/0,008; 1/0,063; 0,33/0,25; 0/0,5; 0/1\}$; $\widetilde{С} = \{0/0,008; 0,25/0,063; 1/0,25; 0,5/0,5; 0/1\}$; $\widetilde{Б} = \{0/0,008; 0/0,063; 0,5/0,25; 1/0,5; 0,75/1\}$; $\widetilde{ОБ} = \{0/0,008; 0/0,063; 0/0,25; 0,83/0,5; 1/1\}$.

Для формирования лингвистических эталонов необходимо чтобы для $\forall T_{КОП}^i$ было справедливо отношение порядка, например, при $i=1, \forall x_{ОМ}: x_{ОМ_k} < x_{ОМ_{k+1}}$. Далее полученные $T_{КВК}$ для НЧ $\widetilde{X} = \{\mu_1/x_1; \dots \mu_i/x_i; \dots \mu_n/x_n\}$ представляются в приведенной форме [1]

$$T_{КОП}^e = \bigcup_{i=1}^5 T_{КОП}^{ei} = \{\widetilde{ОМ}^e, \widetilde{М}^e, \widetilde{С}^e, \widetilde{Б}^e, \widetilde{ОБ}^e\}, \quad \text{где } \widetilde{ОМ}^e = \{0/0,008; 1/0,008; 0,25/0,063; 0/0,25\};$$

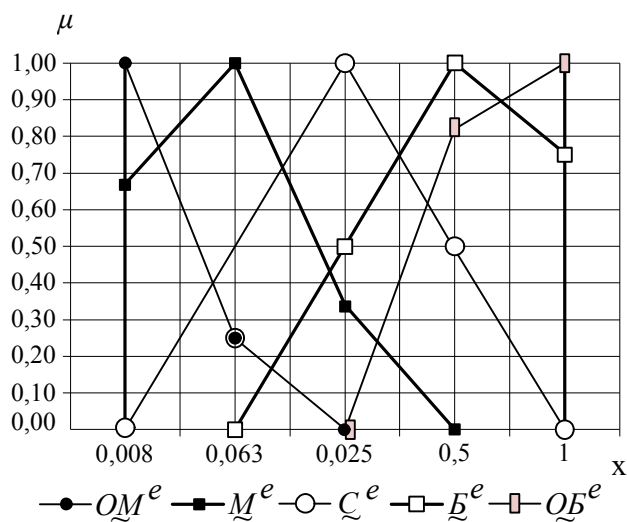


Рис. 3. Лингвистические эталоны НЧ для КОП

$$\begin{aligned} \underline{M}^e &= \{0/0,008; 0,67/0,008; 1/0,063; 0,33/0,25; \\ &0/0,5\}; \underline{C}^e = \{0/0,008; 0,25/0,063; 1/0,25; 0,5 \\ &/0,5; 0/1\}; \underline{B}^e = \{0/0,063; 0,5/0,25; 1/0,5; \\ &0,75/1; 0/1\}; \underline{OB}^e = \{0/0,25; 0,83/0,5; 1/1; 0/1\}. \end{aligned}$$

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

С учетом проведенного эксперимента модель эталонов для $\langle CO_2, T_{CO_2}, U_{CO_2} \rangle$ построим на основе базового термножества с тремя нечеткими термами:

$T_{CO_2} = \bigcup_{i=1}^3 T_{CO_2}^i = \{ \text{“НИЗКАЯ” (Н), “СРЕДНЯЯ” (С), “ВЫСОКАЯ” (В)} \}$, которые могут быть отображены на универсальное множество $U_{CO_2} \in \{0, \max_{CO_2}\}$.

Данные для T_{CO_2} 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 $\max_{CO_2} = 100$, отражающее усредненное значение количества пакетов с сети Internet, полученное с помощью стресс-теста.

Формируем матрицу подсказок по формуле

$$\|k_j\| = \left\| \bigcup_{j=1}^3 \sum_{i=1}^3 b_{ij} \right\| = \|4, 4, 5\|, \text{ где } b_{ij} - \text{элементы эмпирических данных (см. табл. 2), которые}$$

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 $cm_i = \bigcup_{j=1}^3 \bigvee_{i=1}^3 c_{ij} = \{3,75; 2,5; 4\}$.

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 $\bigcup_{i=1}^3 \Delta B_i / B = \{0,05; 0,25; 1\}$

($\Delta B/B$ – отклонение параметра $\Delta B_{CO_2} \in [0, B_{CO_2}]$, а B_{CO_2} – максимально возможное значение, которое характеризует текущие измерения) и получаем НЧ: $\underline{H} = \{1/0,05; 0,33/0,25; 0/1\}$;

$$\underline{C} = \{0,5/0,05; 0,9/0,25; 0,4/1\}; \underline{B} = \{0/0,05; 0,31/0,25; 1/1\}.$$

Учитывая, что для $\forall T_{CO_2}^i$ справедливо отношение порядка, например, при $i=1, \forall x_M$: $x_{H_k} < x_{H_{k+1}}$. Полученные T_{CO_2} для НЧ $\underline{X} = \{\mu_1/x_1; \dots; \mu_i/x_i; \dots; \mu_n/x_n\}$ представляются в приведенной форме [1] $T_{CO_2}^e = \bigcup_{i=1}^3 T_{CO_2}^{ei} = \{ \underline{H}^e, \underline{C}^e, \underline{B}^e \}$, где $\underline{H}^e = \{0/0,05; 1/0,05; 0,33/0,25; 0/1\}$;

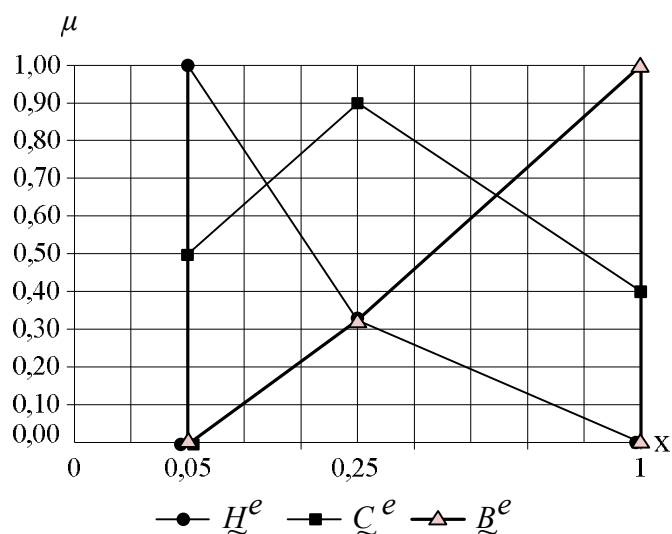


Рис. 4 Эталонные НЧ для CO₂

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

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

Полученные значения и будут использоваться в качестве эталонных для CO₂, графическое изображение которых представлено на рис. 4.

По аналогии с CO₂ проведем вычисления для $\langle Z_{M3}, T_{Z_{M3}}, U_{Z_{M3}} \rangle$ с использованием терм-множества на три нечетких терма: $T_{Z_{M3}} = \bigcup_{i=1}^3 T_{Z_{M3}}^i = \{ \text{“МАЛАЯ” (M), “СРЕДНЯЯ” (C), “ВЫСОКАЯ” (B)} \}$, которые отображаются на универсальное множество $U_{Z_{M3}} \in \{0, \max_{Z_{M3}}\}$.

Данные для $T_{Z_{M3}}$ Таблица 3

Значения ЛП	Интервал		
	N1	N2	N3
M	3	1	0
C	1	3	2
B	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 $\max_{Z_{M3}} = 1000$ 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 $ct_i = \bigcup_{j=1}^3 \bigvee_{i=1}^3 c_{ij} = \{5,25; 3,5;$

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 $\Delta B_{Z_{M3}} \in [0, B_{Z_{M3}}]$, а $B_{Z_{M3}}$ – максимально возможное значение, которое характеризует текущие измерения) и получаем НЧ: $\underline{M} = \{1/0,01; 0,33/0,1; 0/1\}$;

$$\underline{C} = \{0,33/0,01; 1/0,1; 0,67/1\}; \underline{B} = \{0/0,01; 0,4/0,1; 1/1\}.$$

При формировании эталонов для $\forall T_{3МЗ}^i$ также справедливо отношение порядка, например, при $i=1, \forall x_M: x_{M_k} < x_{M_{k+1}}$. Далее $T_{3МЗ}$ для НЧ $\underline{X} = \{\mu_1/x_1; \dots; \mu_i/x_i; \dots; \mu_n/x_n\}$ представляются в приведенной форме [1] $T_{3МЗ}^e = \bigcup_{i=1}^3 T_{3МЗ}^{ei} = \{M^e, C^e, B^e\}$, где $M^e = \{0/0,01; 1/$

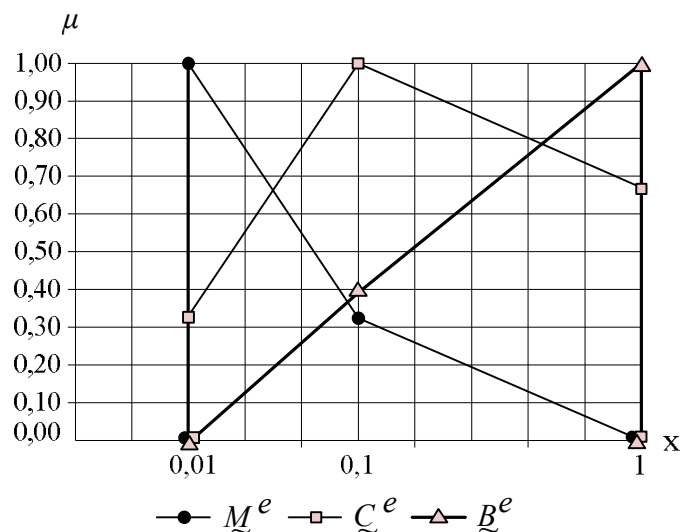


Рис. 5. Эталонные НЧ для ЗМЗ

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

$$\|k_j\| = \left\| \bigcup_{j=1}^3 \sum_{i=1}^3 b_{ij} \right\| = \|4,7,5\|, \text{ где } b_{ij} - \text{элементы эмпирических данных (см. табл. 4), которые}$$

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

А також, формуючи еталони для $\forall T_{КПОА}^i$ справедливо відношення порядку, наприклад, при $i=1$, $\forall x_M: x_{M_k} < x_{M_{k+1}}$. Далі отримані $T_{КПОА}$ для НЧ $\underline{X} = \{\mu_1/x_1; \dots \mu_i/x_i; \dots \mu_n/x_n\}$ представляються в приведеній формі [1] $T_{КПОА}^e = \bigcup_{i=1}^3 T_{КПОА}^{ei} = \{M^e, C^e, B^e\}$, де $M^e = \{0/0,01;$

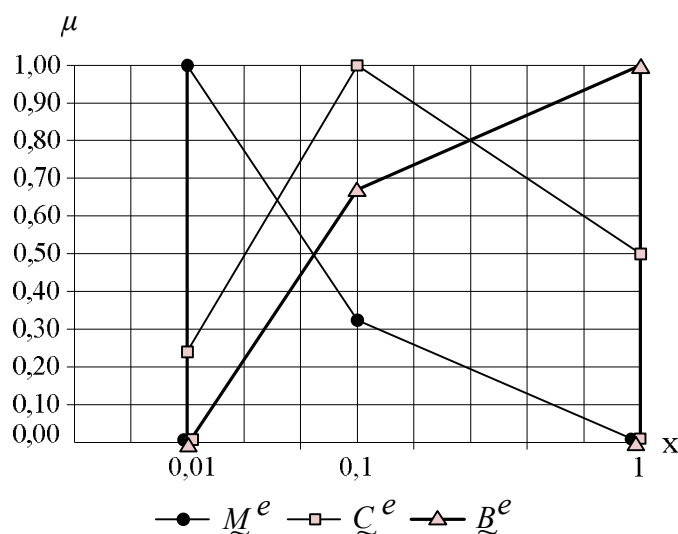


Рис. 6. Еталонні НЧ для КПОА

конкретні еталонні НЧ, які необхідні для формування логічних правил, що дозволяють підвищити ефективність відповідних засобів безпеки, заснованих на ідентифікації аномального стану в ІС.

ЛИТЕРАТУРА

1. Корченко А.Г. Побудова систем захисту інформації на нечітких множинах : Теорія і практичні рішення / А.Г.Корченко. – К. : МК-Пресс, 2006. – 320 с.
2. Стасюк А.І., Корченко А.А. Базова модель параметрів для побудови систем виявлення атак / А.І. 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 / А. 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.

