ЛІТЕРАТУРА

1. Ленков С.В. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А. – К.: Арий, 2008.
2. Горелик В.А. Исследование операций / Горелик В.А., Ушаков И.А. – М.: Машиностроение, 1986. – 288 с.
3. Вунш Г. Теория систем / Вунш Г. – М.: Сов. радио, 1978. – 288 с.
4. Тиснина Е.О. Абсолютная устойчивость положения равновесия системы поддержки принятия решений в системе защиты информации / Тиснина Е.О., Хорошко В.А. // Сучасний захист інформації, №4, 2010. – С. 74-79.
5. Мину М. Математическое программирование. Теория и алгоритмы / Мину М. – М.: Наука, 1990. – 488 с.
6. Хоменюк В.В. Элементы теории многоцелевой оптимизации / Хоменюк В.В. – М.: Наука, 1983. – 343 с.
7. Игнатов В.А. Аксиоматическая теория математического моделирования критериев оптимальности и ограничений / Игнатов В.А., Минаев Ю.Н., Гузий Н.Н. // Захист інформації, №4, 2005. – С. 46-56.

Надійшла: 22.10.2012 р.

Рецензент: д.т.н., професор Щербак Л.М.

УДК 004.056.53(045)

Корченко А.А.

МОДЕЛЬ ЭВРИСТИЧЕСКИХ ПРАВИЛ НА ЛОГИКО-ЛИНГВИСТИЧЕСКИХ СВЯЗКАХ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Недостатком современных систем обнаружения вторжений, построенных на принципе идентификации аномального состояния является то, что они в основном ориентированы на использование таких математических моделей, которые требуют много времени на подготовку статистических данных. Математические модели, основанные на экспертных подходах в этом отношении являются более эффективными, но для выполнения своих функций необходимо использование соответствующих решающих правил. Для решения этой задачи в работе предложена модель эвристических правил на нечеткой логике, которая за счет использования множества пар "атака $\rightarrow$ параметры" и "атака $\rightarrow$ набор логико-лингвистических связок", а также универсальной модели эталонов параметров позволяет отображать аномальное состояние, порождаемое определенным типом кибератак в компьютерной сети. На основе этой модели были разработаны примеры правил для обнаружения сканирования, спуфинга и Dos-атак, которые могут практически использоваться для усовершенствования реальных систем выявления аномалий порожденных атакующими действиями в компьютерных системах.

Ключевые слова: кибератака, системы обнаружения вторжений, атака в компьютерных системах, аномалия в сетевом трафике, обнаружение аномалий в компьютерных системах, логико-лингвистическая связка, эвристические правила, экспертная оценка.

Стремительное развитие информационных технологий (ИТ) в свою очередь породило большое количество угроз ресурсам информационных систем (РИС). Одним из решений обеспечения безопасности РИС, являются системы обнаружения вторжений (СОВ) представляющие собой программные или аппаратные средства, ориентированные прежде всего на выявление фактов неавторизованного доступа. Следует отметить, что современные СОВ основываются на сигнатурном (шаблонном) и аномальном принципах.

Первый базируется на представлении каждой атаки в виде определенного шаблона (модели, сценария, правила, сигнатуры) отражающего характеристики и сценарии возможных вторжений. Поэтому такие системы с достаточно высокой точностью выявляют тип кибератак и практически функционируют без ложных срабатываний. Анализ сетевого трафика с использованием сигнатурного принципа характерен тем, что распознавание возможно только при известных кибератаках, а для этого необходимо постоянно обновлять и расширять наборы шаблонов. Кроме неустойчивости к новейшим типам вторжений, такие системы сильно зависят от скорости разработки и обновления сигнатур. Также известно, что для сложных распределенных атак проверка известных шаблонов является достаточно сложной задачей.

Второй принцип основан на выявлении аномального состояния системы порожденного кибератакой и ориентирован на контроль активности в среде окружения, например, наблюдение за параметрами сетевого трафика. Преимущества систем,

реализирующих этот принцип, в первую очередь связано с тем, что они могут обнаруживать не только новые виды кибератак, но и те, которые характеризуются большой продолжительностью во времени.

Существующие СОВ аномального принципа в основном ориентированы на использование таких математических моделей, которые требуют много времени на подготовку статистических данных, что не требуют более эффективные в этом отношении экспертные подходы, преимущества которых показаны в [1]. В связи с этим актуальной задачей при разработке СОВ является создание моделей обнаружения аномалий на основе экспертных оценок. В работе [2] предложена базовая модель параметров (БМП), которая за счет множества пар "атака $\rightarrow$ параметры" и "атака $\rightarrow$ набор лингвистических связок" позволяют отображать аномальное состояние, порождаемое определенным типом кибератак в компьютерной сети. Также, известна универсальная модель эталонов (УМЭ) [3], которая за счет данных экспертных оценок и БМП позволяет формировать множества эталонов лингвистических переменных характерных для определенного типа атак.

Применение этих моделей при построении СОВ, базирующихся на втором принципе, связано с необходимостью формирования правил, направленных на выявления аномального состояния порожденного атакующими действиями. В связи с этим, целью данной работы является разработка математической модели используемой при формировании соответствующих эвристических правил для идентификации аномального состояния в среде окружения. Под средой окружения будем подразумевать совокупность значений сформированных переменных (например, время обработки запроса, загруженность процессора, количество обращений к ресурсу, число подключений и др.), которые можно использовать для оценивания протекающих процессов в информационной системе (ИС) с целью выявления ее аномального состояния. Отображением среды окружения в данном случае могут быть параметры входящие в множество $\boldsymbol{P}$ [2]. Для решения поставленной задачи необходимо построить эвристические правила, представляющие собой некоторые утверждения, основанные на результате обобщения определенных теоретических и экспериментальных знаний (данных) и отражающие интуитивное суждение лица, принимающего решение, для обеспечения поиска рационального смыслового решения слабоформализованных задач.

Построение эвристических правил можно осуществить с помощью соответствующей модели, для создания которой введем множество лингвистических идентификаторов

$$\boldsymbol{LI}=\bigcup_{i=1}^{d} LI_i = \{LI_1, LI_2, \ldots, LI_d\}, \quad (1)$$

где d – количество элементов множества, необходимое для отображения аномального состояния, а LI_i $(i=\overline{1,d})$ – элементы $\boldsymbol{LI}$, каждый из которых принимает одно из текстовых значений, характеризующих в лингвистической форме уровень аномального состояния системы, которое может быть порождено атакующими действиями. Например, при $d=5$ выражение (1) можно определить как:

$$\boldsymbol{LI}=\bigcup_{i=1}^{5} LI_i = \{LI_1, LI_2, LI_3, LI_4, LI_5\}=\{Н, БНВ, БВН, В, П\}, \quad (2)$$

где $LI_1=Н$, $LI_2=БНВ$, $LI_3=БВН$, $LI_4=В$ и $LI_5=П$ соответственно отображаются текстовыми значениями "Низкий", "Больше низкий чем высокий", "Больше высокий чем низкий", "Высокий" и "Предельный".

Далее на основе множеств идентификаторов **LI** и набора лингвистических или с расширенным названием – логико-лингвистических связок **LC** построим множество эвристических правил

$$\boldsymbol{ER}=\{\bigcup_{i=1}^{n} \boldsymbol{ER_i}\}=\{\boldsymbol{ER_1}, \boldsymbol{ER_2}, \ldots, \boldsymbol{ER_n}\}, \quad (3)$$

где $\boldsymbol{ER_i}$ $(i=\overline{1,n})$ – подмножество возможных правил для выявления i-го аномального состояния, порожденного i-й атакой, при этом

$$\bigcup_{i=1}^{n} \boldsymbol{ER_i} = \bigcup_{i=1}^{n}\{\bigcup_{j=1}^{r_n} ER_{ij}\} = \{ER_{11}, ER_{12}, \ldots, ER_{1r_1}\},$$
$$\{ER_{21}, ER_{22}, \ldots, ER_{2r_2}\}, \ldots, \{ER_{n1}, ER_{n2}, \ldots, ER_{nr_n}\}, \quad (4)$$

где ER_{ij} $(i=\overline{1,n},\ j=\overline{1,r_n})$ – j-е правило i-го подмножества возможных правил, а r_i $(i=\overline{1,n})$ – общее количество возможных правил, направленных на обнаружение i-й аномалии.

Отметим, что каждому ER_{ij} соответствует эвристическое выражение (правило) т.е.:

$$\begin{aligned}
&\{ER_{11}=(LC_{11}\rightarrow LI_{11}),\quad ER_{12}=(LC_{12}\rightarrow LI_{12}),\ \ldots,\quad ER_{1r_1}=(LC_{1r_1}\rightarrow LI_{1r_1})\},\\
&\{ER_{21}=(LC_{21}\rightarrow LI_{21}),\quad ER_{22}=(LC_{22}\rightarrow LI_{22}),\ \ldots,\quad ER_{2r_2}=(LC_{2r_2}\rightarrow LI_{2r_2})\},\\
&\qquad\qquad\ldots\\
&\{ER_{n1}=(LC_{n1}\rightarrow LI_{n1}),\quad ER_{n2}=(LC_{n2}\rightarrow LI_{n2}),\ \ldots,\quad ER_{nr_n}=(LC_{nr_n}\rightarrow LI_{nr_n})\}.
\end{aligned} \quad (5)$$

Обобщая выражение (5) с учетом (3) и (4) получим

$$\boldsymbol{ER}=\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{r_i} ER_{ir_j}\}=\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{r_i}(LC_{ir_j}\rightarrow LI_{ir_j})\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{r_i} ER_{ir_j}=(LC_{ir_j}\rightarrow LI_{ir_j})\}\}, \quad (6)$$

где ER_{ir_j} есть r_j-е правило выявления аномалии порожденной i-й атакой, которое буквально интерпретируется как: “Если LC_{ir_j} истинно, то уровень аномального состояния, который может быть порожден i-й атакой, будет LI_{ir_j}”.

Построение правил обычно осуществляется на основе экспертного подхода, особенно это важно в тех случаях, когда необходимо дать предпочтение одной из альтернатив, например, при каком LC_{ir_j} (6) исход, связанный с LI_{ir_j} будет наиболее объективно отображать состояние системы. Рассмотрим процесс формирования предпочтения для набора альтернатив на конкретном примере.

Пусть для построения подмножества правил $\boldsymbol{ER_1}$ используется r_1 логико-лингвистических связок и d (1) лингвистических идентификаторов, один из которых наиболее объективно может отразить состояние среды окружения относительно наличия аномалии. Итак, общее количество возможных альтернативных решений – $d \times r_1$, т.е. на составление каждого правила ER_{1j} $(j=\overline{1,r_1})$ необходимо рассмотреть d альтернативных вариантов правил, для выбора одного из которых воспользуемся методами определения коэффициентов важности (КВ) [4]. Воспользуемся методом ранговых преобразований (РП), поскольку он позволяет воспользоваться услугами нескольких экспертов, в качестве входных данных применяются табличные формы, выходная функция линейная, а трудоемкость низкая (см. табл. в [4]).

Далее, в качестве примера, определим $d=r_1=5$, тогда $\boldsymbol{LC_1}=\{\bigcup_{j=1}^{r_1} LC_{1j}\}=\{LC_{11}, LC_{12}, LC_{13}, LC_{14}, LC_{15}\}=\{((\underset{\sim}{t}_{СОЗ}\cong\underset{\sim}{H}^{e}\vee\underset{\sim}{t}_{ЗЗМ}\cong\underset{\sim}{H}^{e})\wedge\underset{\sim}{t}_{КОП}\cong\underset{\sim}{ОМ}^{e}),((\underset{\sim}{t}_{СОЗ}\cong\underset{\sim}{H}^{e}\vee\underset{\sim}{t}_{ЗЗМ}\cong\underset{\sim}{H}^{e})\wedge\underset{\sim}{t}_{КОП}\cong\underset{\sim}{M}^{e}),((\underset{\sim}{t}_{СОЗ}\cong\underset{\sim}{H}^{e}\vee\underset{\sim}{t}_{ЗЗМ}\cong\underset{\sim}{H}^{e})\wedge\underset{\sim}{t}_{КОП}\cong\underset{\sim}{C}^{e}),((\underset{\sim}{t}_{СОЗ}\cong\underset{\sim}{H}^{e}\vee\underset{\sim}{t}_{ЗЗМ}\cong\underset{\sim}{H}^{e})\wedge\underset{\sim}{t}_{КОП}\cong\underset{\sim}{Б}^{e}),((\underset{\sim}{t}_{СОЗ}\cong\underset{\sim}{H}^{e}\vee\underset{\sim}{t}_{ЗЗМ}\cong\underset{\sim}{H}^{e})\wedge\underset{\sim}{t}_{КОП}\cong\underset{\sim}{ОБ}^{e})\}$, а в качестве значений LI_{1j} $(j=\overline{1,5})$ воспользуемся данными из формулы (2). Таким образом, для каждого LC_{1j} $(j=\overline{1,5})$ возможны $d=5$ исходов выявления аномалий, связанных с конкретными значениями лингвистических идентификаторов в (2). Наиболее объективный из исходов определим с помощью метода СР [4].

Согласно этого метода, в качестве примера, воспользуемся суждениями 4-х экспертов относительно $d=5$ возможных исходов ER^{k}_{1j} $(k=\overline{1,d},\ j=\overline{1,r_1})$ по каждому j-му правилу.

Например, для первого правила подмножество альтернативных решений будет $\bigcup_{k=1}^{d} ER_{11}^{k} = \{$ ER_{11}^{1}, ER_{11}^{2}, ER_{11}^{3}, ER_{11}^{4}, $ER_{11}^{5}\} =$ $\{((t_{СОЗ} \cong \underset{\sim}{H}^{e} \vee \underset{\sim}{t}_{ЗЗМ} \cong \underset{\sim}{H}^{e}) \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{OM}^{e}) \to Н$, $((\underset{\sim}{t}_{СОЗ} \cong \underset{\sim}{H}^{e} \vee \underset{\sim}{t}_{ЗМЗ} \cong \underset{\sim}{H}^{e}) \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{OM}^{e}) \to БНВ$, $((\underset{\sim}{t}_{СОЗ} \cong \underset{\sim}{H}^{e} \vee \underset{\sim}{t}_{ЗМЗ} \cong \underset{\sim}{H}^{e}) \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{OM}^{e}) \to БВН$, $((\underset{\sim}{t}_{СОЗ} \cong \underset{\sim}{H}^{e} \vee \underset{\sim}{t}_{ЗМЗ} \cong \underset{\sim}{H}^{e}) \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{OM}^{e}) \to В$, $((\underset{\sim}{t}_{СОЗ} \cong \underset{\sim}{H}^{e} \vee \underset{\sim}{t}_{ЗМЗ} \cong \underset{\sim}{H}^{e}) \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{OM}^{e}) \to П\}$.

Таблица 1

Ранги ER_{1j}^{k} и КВ

ER_{1j}^{k}	j	k	Эксперты				x_{1j}^{k}	λ_{1j}^{k}
			1	**2**	**3**	**4**		
ER_{11}^{1}	1	1	1	3	1	2	1,75	0,18
ER_{11}^{2}		2	2	1	3	2	2	0,2
ER_{11}^{3}		3	3	2	2	2	2,25	0,23
ER_{11}^{4}		4	2	4	3	3	3	0,3
ER_{11}^{5}		5	4	4	3	4	3,75	0,38
ER_{12}^{1}	2	1	2	3	1	2	2	0,2
ER_{12}^{2}		2	1	2	1	2	1,5	0,15
ER_{12}^{3}		3	3	1	2	3	2,25	0,23
ER_{12}^{4}		4	3	4	2	2	2,75	0,28
ER_{12}^{5}		5	3	2	3	4	3	0,3
ER_{13}^{1}	3	1	2	3	2	4	2,75	0,28
ER_{13}^{2}		2	3	2	2	1	2	0,2
ER_{13}^{3}		3	2	3	1	1	1,75	0,18
ER_{13}^{4}		4	3	4	3	4	3,5	0,35
ER_{13}^{5}		5	4	3	2	4	3,25	0,33
ER_{14}^{1}	4	1	4	2	2	4	3	0,3
ER_{14}^{2}		2	2	4	3	2	2,75	0,28
ER_{14}^{3}		3	3	1	2	2	2	0,2
ER_{14}^{4}		4	1	2	3	1	1,75	0,18
ER_{14}^{5}		5	2	4	4	3	3,25	0,33
ER_{15}^{1}	5	1	4	4	3	3	3,5	0,35
ER_{15}^{2}		2	2	4	4	3	3,25	0,33
ER_{15}^{3}		3	2	4	3	3	3	0,3
ER_{15}^{4}		4	4	3	2	3	3	0,3
ER_{15}^{5}		5	2	2	4	3	2,75	0,28

Далее на основе РП определим КВ, которые отражаются параметром λ. Его минимальное значение свидетельствует о большей предпочтительности альтернативы, т.е. ее КВ более высокий. Для правила ER_{11} произведем расчеты значений x_{1j}^{k} и λ_{1j}^{k} по каждому из возможных исходов ER_{11}^{k} $(k = \overline{1,5})$: x_{11}^{1}=(1+3+1+2)/4=1,75; x_{11}^{2}=(2+1+3+2)/4=2; x_{11}^{3}=(3+2+2+2)/4=2,25; x_{11}^{4}=(2+4+3+3)/4=3; x_{11}^{5}=(4+4+3+4)/4=3,75. Значение КВ определяется как $\lambda_{1j}^{k} = x_{1j}^{k} / N$, где N – сумма всех рангов ($N=10$). По результатам, занесенным в табл. 1 видно, что лучший исход имеет, ER_{11}^{1} поскольку $\bigwedge_{k=1}^{5} \lambda_{11}^{k} = \lambda_{11}^{1} = 0{,}18$.

Аналогично произведем расчеты для ER_{1j}^{k} $(j = \overline{2,5})$: ER_{12}^{k} – x_{12}^{1}=(2+3+1+2)/4=2; x_{12}^{2}=(1+2+1+2)/4=1,5; x_{12}^{3}=(3+1+2+3)/4=2,25; x_{12}^{4}=(3+4+2+2)/4=2,75; x_{12}^{5}=(3+2+3+4)/4=3; ER_{13}^{k} – x_{13}^{1}=(2+3+2+4)/4=2,75; x_{13}^{2}=(3+2+2+1)/4=2; x_{13}^{3}=(2+3+1+1)/4=1,75; x_{13}^{4}=(3+4+3+4)/4=3,5; x_{13}^{5}=(4+3+2+4)/4=3,25; ER_{14}^{k} – x_{14}^{1}=(4+2+2+4)/4=3; x_{14}^{2}=(2+4+3+2)/4=2,75; x_{14}^{3}=(3+1+2+2)/4=2; x_{14}^{4}=(1+2+3+1)/4=1,75; x_{14}^{5}=(2+4+4+3)/4=3,25; ER_{15}^{k} – x_{15}^{1}=(4+4+3+3)/4=3,5; x_{15}^{2}=(2+4+4+3)/4=3,25; x_{15}^{3}=(2+4+3+3)/4=3; x_{15}^{4}=(4+3+2+3)/4=3; x_{15}^{5}=(2+2+4+3)/4=2,75.

По результатам вычислений (см. табл. 1) видно, что лучший исход для правил ER_{12}, ER_{13}, ER_{14}, ER_{15} имеют соответственно альтернативные варианты ER_{12}^{2}, ER_{13}^{3}, ER_{14}^{4}, ER_{15}^{5}.

Полученные данные можно использовать в качестве конкретных значений при построении реальных правил в практических СОВ. С этой целью, с учетом (6), осуществим структурирование необходимых данных путем ввода матриц инициализации (МІ) для множеств ***LI*** и ***LC***, которые обозначим соответственно $LI(n, r_n)$ и $LC(n, r_n)$, т.е.

$$LI(n, r_n)=\begin{Vmatrix} LI(1,1), LI(1,2), \ldots, LI(1,r_n) \\ LI(2,1), LI(2,2), \ldots, LI(2,r_n) \\ \ldots \\ LI(n,1), LI(n,2), \ldots, LI(n,r_n) \end{Vmatrix} \quad LC(n, r_n)=\begin{Vmatrix} LC(1,1), LC(1,2), \ldots, LC(1,r_n) \\ LC(2,1), LC(2,2), \ldots, LC(2,r_n) \\ \ldots \\ LC(n,1), LC(n,2), \ldots, LC(n,r_n) \end{Vmatrix}. \quad (7)$$

Например, при n=3 и r_n=5 на основе экспертных оценок [4] были определены следующие MI $LI(3, 5)$ и $LC(3, 5)$, т.е.

$$LI(3,5)=\begin{Vmatrix} Н & БНВ & БВН & В & П \\ Н & Н & БВН & В & П \\ Н & БНВ & БВН & В & В \end{Vmatrix} \text{ и}$$

$$LC(3,5)=\begin{Vmatrix} (\underset{\sim}{t}_{СОЗ} \cong \underset{\sim}{H}^e \vee & (\underset{\sim}{t}_{СОЗ} \cong \underset{\sim}{H}^e \vee & (\underset{\sim}{t}_{СОЗ} \cong \underset{\sim}{H}^e \vee & (\underset{\sim}{t}_{СОЗ} \cong \underset{\sim}{H}^e \vee & (\underset{\sim}{t}_{СОЗ} \cong \underset{\sim}{H}^e \vee \\ \underset{\sim}{t}_{ЗЗМ} \cong \underset{\sim}{H}^e) \wedge & \underset{\sim}{t}_{ЗЗМ} \cong \underset{\sim}{H}^e) \wedge & \underset{\sim}{t}_{ЗЗМ} \cong \underset{\sim}{H}^e) \wedge & \underset{\sim}{t}_{ЗЗМ} \cong \underset{\sim}{H}^e) \wedge & \underset{\sim}{t}_{ЗЗМ} \cong \underset{\sim}{H}^e) \wedge \\ \underset{\sim}{t}_{КОП} \cong \underset{\sim}{ОМ}^e & \underset{\sim}{t}_{КОП} \cong \underset{\sim}{М}^e & \underset{\sim}{t}_{КОП} \cong \underset{\sim}{С}^e & \underset{\sim}{t}_{КОП} \cong \underset{\sim}{Б}^e & \underset{\sim}{t}_{КОП} \cong \underset{\sim}{ОБ}^e \\ \underset{\sim}{t}_{КПОА} \cong \underset{\sim}{Б}^e \wedge & \underset{\sim}{t}_{КПОА} \cong \underset{\sim}{Б}^e \wedge & \underset{\sim}{t}_{КПОА} \cong \underset{\sim}{Б}^e \wedge & \underset{\sim}{t}_{КПОА} \cong \underset{\sim}{Б}^e \wedge & \underset{\sim}{t}_{КПОА} \cong \underset{\sim}{Б}^e \wedge \\ \underset{\sim}{t}_{КОП} \cong \underset{\sim}{ОМ}^e & \underset{\sim}{t}_{КОП} \cong \underset{\sim}{М}^e & \underset{\sim}{t}_{КОП} \cong \underset{\sim}{С}^e & \underset{\sim}{t}_{КОП} \cong \underset{\sim}{Б}^e & \underset{\sim}{t}_{КОП} \cong \underset{\sim}{ОБ}^e \\ \underset{\sim}{t}_{ВВК} \cong \underset{\sim}{М}^e \wedge & \underset{\sim}{t}_{ВВК} \cong \underset{\sim}{М}^e \wedge & \underset{\sim}{t}_{ВВК} \cong \underset{\sim}{М}^e \wedge & \underset{\sim}{t}_{ВВК} \cong \underset{\sim}{М}^e \wedge & \underset{\sim}{t}_{ВВК} \cong \underset{\sim}{М}^e \wedge \\ \underset{\sim}{t}_{КВК} \cong \underset{\sim}{ОМ}^e & \underset{\sim}{t}_{КВК} \cong \underset{\sim}{М}^e & \underset{\sim}{t}_{КВК} \cong \underset{\sim}{С}^e & \underset{\sim}{t}_{КВК} \cong \underset{\sim}{Б}^e & \underset{\sim}{t}_{КВК} \cong \underset{\sim}{ОБ}^e \end{Vmatrix}, \quad (8)$$

где $\underset{\sim}{t}_{КОП}$, $\underset{\sim}{t}_{СОЗ}$, $\underset{\sim}{t}_{ЗЗМ}$, $\underset{\sim}{t}_{КПОА}$, $\underset{\sim}{t}_{ВВК}$, $\underset{\sim}{t}_{КВК}$ – текущие значения параметров КОП (Количество одновременных подключений), СОЗ (Скорость обработки запросов), ЗМЗ (Задержка между запросами), КПОА (Количество пакетов с одинаковым адресом отправителя и получателя), ВВК (Возраст виртуального канала), КВК (Количество виртуальных каналов) и являются идентификаторами параметров [2] в среде окружения. Используемый в (8) знак "$\cong$" – интерпретируется как "Нечеткое равно" и указывает на то, что текущее значение параметра (например, $\underset{\sim}{t}_{СОЗ}$) находящегося слева от "$\cong$" наиболее близко к одному из элементов (например, $\underset{\sim}{H}^e$) из заданного множества (например, $T^e_{СОЗ}$ ={ $\underset{\sim}{H}^e$, $\underset{\sim}{C}^e$, $\underset{\sim}{B}^e$ }), который указывается справа от "$\cong$", т.е. запись $\underset{\sim}{t}_{СОЗ} \cong \underset{\sim}{H}^e$ можно интерпретировать как: "$\underset{\sim}{t}_{СОЗ}$ наиболее близко расположен к $\underset{\sim}{H}^e$ входящего в $T^e_{СОЗ}$".

Далее с учетом MI (при i=1, $j=\overline{1,5}$) для $LI(n, r_n)$ и $LC(n, r_n)$ на основе (7) и (8) построим подмножество правил $\boldsymbol{ER_1}$ для выявления аномального состояния, которое может быть порождено Dos (DDos) атакой.

Отметим, что правило ER_{15} в (9) буквально можно интерпретировать как: “Если $\underset{\sim}{t}_{СОЗ} \cong \underset{\sim}{Н}^{e}$ или $\underset{\sim}{t}_{ЗЗМ} \cong \underset{\sim}{Н}^{e}$ и при этом $\underset{\sim}{t}_{КОП} \cong \underset{\sim}{ОБ}^{e}$, то уровень аномального состояния, который может быть порожден Dos-атакой, будет ПРЕДЕЛЬНЫЙ”.

$$\boldsymbol{ER_1} = \left\{ \begin{array}{l} ER_{11} = ((\underset{\sim}{t}_{СОЗ} \cong \underset{\sim}{Н}^{e} \vee \underset{\sim}{t}_{ЗЗМ} \cong \underset{\sim}{Н}^{e}) \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{ОМ}^{e}) \to Н, \\ ER_{12} = ((\underset{\sim}{t}_{СОЗ} \cong \underset{\sim}{Н}^{e} \vee \underset{\sim}{t}_{ЗЗМ} \cong \underset{\sim}{Н}^{e}) \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{М}^{e}) \to БНВ, \\ ER_{13} = ((\underset{\sim}{t}_{СОЗ} \cong \underset{\sim}{Н}^{e} \vee \underset{\sim}{t}_{ЗЗМ} \cong \underset{\sim}{Н}^{e}) \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{С}^{e}) \to БВН, \\ ER_{14} = ((\underset{\sim}{t}_{СОЗ} \cong \underset{\sim}{Н}^{e} \vee \underset{\sim}{t}_{ЗЗМ} \cong \underset{\sim}{Н}^{e}) \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{Б}^{e}) \to В, \\ ER_{15} = ((\underset{\sim}{t}_{СОЗ} \cong \underset{\sim}{Н}^{e} \vee \underset{\sim}{t}_{ЗЗМ} \cong \underset{\sim}{Н}^{e}) \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{ОБ}^{e}) \to П \end{array} \right\}. \quad (9)$$

Из подмножества правил (9) видно, что для каждой логико-лингвистической связки из ER_{1j} $(j = \overline{1,5})$ определены конкретные значения из $\boldsymbol{LI}$ согласно расчетов КВ с помощью метода РП. Используя эти данные по аналогии можно составить правила для выявления аномалий порожденных спуфингом и сканированием [2, 3]. Так с учетом (7) и (8) при $i = \overline{2,3}$ и $j = \overline{1,5}$ наборы правил $\boldsymbol{ER_2}$ (10) и $\boldsymbol{ER_3}$ (11) будут иметь следующий вид:

$$\boldsymbol{ER_2} = \{ ER_{21} = (\underset{\sim}{t}_{КПОА} \cong \underset{\sim}{Б}^{e} \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{ОМ}^{e}) \to Н,$$

$$ER_{22} = (\underset{\sim}{t}_{КПОА} \cong \underset{\sim}{Б}^{e} \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{М}^{e}) \to БНВ,\ ER_{23} = (\underset{\sim}{t}_{КПОА} \cong \underset{\sim}{Б}^{e} \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{С}^{e}) \to БВН,$$

$$ER_{24} = (\underset{\sim}{t}_{КПОА} \cong \underset{\sim}{Б}^{e} \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{Б}^{e}) \to В,\ ER_{25} = (\underset{\sim}{t}_{КПОА} \cong \underset{\sim}{Б}^{e} \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{ОБ}^{e}) \to П \} \text{ и} \quad (10)$$

$$\boldsymbol{ER_3} = \{ ER_{31} = (\underset{\sim}{t}_{ВВК} \cong \underset{\sim}{М}^{e} \wedge \underset{\sim}{t}_{КВК} \cong \underset{\sim}{ОМ}^{e}) \to Н,$$

$$ER_{32} = (\underset{\sim}{t}_{ВВК} \cong \underset{\sim}{М}^{e} \wedge \underset{\sim}{t}_{КВК} \cong \underset{\sim}{М}^{e}) \to БНВ,\ ER_{33} = (\underset{\sim}{t}_{ВВК} \cong \underset{\sim}{М}^{e} \wedge \underset{\sim}{t}_{КВК} \cong \underset{\sim}{С}^{e}) \to БВН,$$

$$ER_{34} = (\underset{\sim}{t}_{ВВК} \cong \underset{\sim}{М}^{e} \wedge \underset{\sim}{t}_{КВК} \cong \underset{\sim}{Б}^{e}) \to В,\ ER_{35} = (\underset{\sim}{t}_{ВВК} \cong \underset{\sim}{М}^{e} \wedge \underset{\sim}{t}_{КВК} \cong \underset{\sim}{ОБ}^{e}) \to П \}. \quad (11)$$

Предложенная в работе модель эвристических правил на нечеткой логике, позволяет за счет использования множества пар “атака $\to$ параметры”, “атака $\to$ набор логико-лингвистических связок” и универсальной модели эталонов параметров отображать аномальное состояние, порождаемое определенным типом кибератак в компьютерной сети. На основе этой модели были разработаны примеры правил для обнаружения сканирования, спуфинга и Dos-атак, которые могут практически быть использованы для усовершенствования реальных систем выявления аномалий, порожденных атакующими действиями в компьютерных системах.

ЛИТЕРАТУРА

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

2. 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.
3. 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.
4. 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.

Надійшла: 23.10.2012 р.

Рецензент: д.т.н., професор Дудикевич В.Б.

УДК 004.942

Кряжич О.О.

ЗАДОВОЛЕННЯ ВИМОГ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ УПРАВЛІННЯ ІМПУЛЬСНИМ ВИБУХОПОЖЕЖНИМ ЗАХИСТОМ ХІМІЧНОГО ПІДПРИЄМСТВА

У статті наведені дослідження щодо забезпечення дотримання умов своєчасності, несуперечності та повноти інформації для управління імпульсним вибухопожежним захистом хімічного підприємства. Наведені особливості запропонованого технологічного рішення, визначені процеси моніторингу інформації та забезпечення інформаційної безпеки. Зазначені команди управління та ідентифікації циркулювання інформації в пакеті програмних продуктів.

Ключові слова: інформація, модель, інтеграція, компонент, імпульсний захист, схема, системні вимоги, цикл, управління, ідентифікатор.

Вступ. В сучасній практиці реалізації проектів з забезпечення безпеки оточуючого середовища є актуальною проблема дотримання вимог своєчасності, несуперечності і повноти інформації, які у більшості випадків не можна виконати з рівня підприємства. Щоб вирішити зазначену проблему слід отримати, обробити та проаналізувати дані, які підприємство може мати не в повному обсязі, або не мати зовсім. Так, моделі імпульсного вибухопожежного захисту хімічного підприємства вимагають наявності інформації:

- про хімічне підприємство, включаючи дані про стан основних виробничих фондів, їх рівень зносу, кваліфікацію персоналу, стан та кількість розміщених на підприємстві й у об'єктових пожежних частинах вибухопожежних засобів;
- відносно оточуючого середовища, кількості населення, що проживає у зоні, що підпадає під забруднюючий вплив у випадку аварії, метеоумов;
- щодо безпосередніх особливостей планування об'єкта, розташування технологічного обладнання, кількості потенційно небезпечної хімічної речовини в кожному апараті;
- про події, що вже відбувалися на об'єкті, прийняті рішення, хронологію дій, задіяні засоби та сили, збитки;
- про наявні засоби та сили, за допомогою яких планується локалізувати та ліквідувати аварійну ситуацію у найкоротший термін, витрати на проведення таких робіт, можливі втрати часу та збитки від цього.

Перелічене вимагає інтеграції окремих програмних продуктів та модулів, пов'язаних технологією забезпечення інформацією в режимі реального часу з місця події. Все це визначає актуальність досліджуваної теми.

Метою дослідження є представлення підходу до забезпечення дотримання вимог своєчасності, несуперечності і повноти інформації в управлінні імпульсним вибухопожежним захистом хімічного підприємства.

Основна частина. Для задоволення перелічених вимог до створення інформаційних технологій управління з забезпечення імпульсного вибухопожежного захисту хімічного підприємства запропоновано [1–3] комплекс програмних продуктів та модулів, логічно поєднаних для забезпечення поставленої мети [4]. Основні складові пропонованого комплексу наведені в табл. 1.