С. М. К о в а л е в, **В. П. Т е р н о в о й** (Ростов-на-Дону, РГУПС).
Иммунный подход к выявлению аномалий во временных рядах.

Рассматривается подход к выявлению аномалий во временных рядах (ВР), основанный на методах искусственных иммунных систем. ВР представляется последовательностью $S = S(t_i) = (\overline{s}(t_1), \overline{s}(t_2), \ldots, \overline{s}(t_n))$. Предполагается заданным обучающее множество O, элементами которого являются фрагменты ВР, характеризующие нормальное течение исследуемого или контролируемого процесса. Задан критерий J, на основе которого устанавливается сходство между ВР. Требуется на основе анализа обучающего множества O сформировать описание в виде системы решающих правил, позволяющих классифицировать как «нормальные» все примеры из множества O и «близкие» к ним по критерию J, а ВР, «существенно» отличающиеся от «нормальных», классифицировать как аномалии. Решающие правила будем представлять в виде логических формул.

Иммунологический подход к выявлению аномалий базируется на принципе отрицательного отбора, механизм реализации которого применительно к рассматриваемой задаче дан ниже.

1. Формируется множество $O = \{\text{ВР}_1, \text{ВР}_2, \ldots, \text{ВР}_n)$ из ВР, характеризующих нормальное течение процесса.

2. На основе множества O с использованием методов кластеризации ВР формируется множество «Я»-строк, являющихся представителями обучающего множества O.

3. На основе множества «Я»-строк формируется множество «НЕ-Я»-строк, не соответствующих строкам из множестве «Я»-строк, и выступающее в качестве детекторов аномалий

Механизм отрицательного отбора положен в основу разработки иммунологического метода контроля трафика. В предлагаемом подходе входные данные выступают в роли антигенов и представлены моделями ВР. В качестве антител выступают модели обобщенных образов ВР, имитирующие иммунные клетки организма, с которыми в процессе распознавания связываются контролируемые образы. Антитела представлены в виде логических формул. Алгоритм распознавания реализован на основе интерпретации логической формулы антитела на ВР, описывающим антиген.

Модель антитела представлена последовательной логической формулой.

О п р е д е л е н и е 1. *Темпорально-интервальным событием* (ТИС) называется кортеж $\tau = \langle \Delta q, \Delta t \rangle$, где $\Delta q = [q_n, q_k]$ есть диапазон изменения числовых значений s_i, $\Delta t = [l_n, l_k]$ есть диапазон изменения продолжительностей ТИС.

О п р е д е л е н и е 2. *Последовательным темпоральным высказыванием* (ПТВ) называется последовательность следующих друг за другом ТИС: $W = \tau_1\, rts\, \tau_2\, rts\, \cdots\, rts\, \tau_m$.

О п р е д е л е н и е 3. *Интерпретацией* ПТВ W на ВР S называется такое разбиение S на m следующих друг за другом интервалов $\Sigma = (\delta_1, \delta_2, \ldots, \delta_m)$, что $(\forall s_j \in \delta_i)\,(q_{i_n} \leqslant s_j \leqslant q_{i_k})$.

Нахождение интерпретации ПТС на S является комбинаторной задачей, для решения которой предлагается композиционно-динамический метод.

О п р е д е л е н и е 4. *Темпорально-признаковым графом* для ТИС $\tau_i = \langle \Delta q_i, \Delta t_i \rangle \in W$ называется граф $RT_{\tau_i}(W/S) = \langle S, R \rangle$, определенный на множестве вершин $\mathcal{S} = \{S_i / S_i \in S\}$, связи между которыми определяются отношением R следующим образом:

$$\forall s_r, s_p \in \mathcal{S} R(s_p, s_r) \;\Leftrightarrow\; ([(l)]_{\,i_n} \leqslant r - p \leqslant l_{i_k}) \,\&\, (\forall s_j \in \delta_i)\,(q_{i_n} \leqslant s_j \leqslant q_{i_k}).$$

Для ПТВ W определяется композиционный граф

$$[(RT)]_{\downarrow}(W/S) = [(RT)]_{\downarrow}(\tau_{\downarrow}1)(W/[(S) \circ RT)]_{\downarrow}(\tau_{\downarrow}2)(W/S) \circ \cdots \circ [(RT)]_{\downarrow}(\tau_{\downarrow}m)(W/S)) \cdots),$$

полученный путем композиции темпорально-признаковых графов $RT_{\tau_i}(W/S)$ в порядке их вхождения в ПТВ.

Теорема. *Для* ПТВ W *существует интерпретация на* S *тогда и только тогда, когда в композиционном графе* $RT_{\square}(W/S)$ *имеет место* $R(s_1, s_n) = 1$.

Приведенная теорема положена в основу построения интерпретирующей модели для процедуры иммунного распознавания.

Рассмотренный подход может быть использован для решения широкого круга задач, связанных с обеспечением контроля функционирования компьютерных систем на основе анализа информационных трафиков.