УДК 004.032

НЕПРЕРЫВНАЯ НЕЙРОННАЯ СЕТЬ АРТ ДЛЯ РАСПОЗНАВАНИЯ РЕЖИМОВ ФУНКЦИОНИРОВАНИЯ ДИНАМИЧЕСКИХ ОБЪЕКТОВ

В. Д. Дмитриенко, А. Ю. Заковоротный

ВВЕДЕНИЕ

В настоящее время существуют тысячи различных методов и алгоритмов классификации и распознавания изображений, причем их число все время увеличивается пропорционально взвешенной сумме числа конкретных практических задач и числа исследователей, решающих эти задачи. В связи с этим в теории распознавания образов предпринимаются попытки создания универсальных методов и подходов, позволяющих решать широкие классы задач распознавания. Один из таких подходов связан с использованием искусственных нейронных сетей Их применение для решения различных задач распознавания во многом основывается на том, что традиционные трудности решения рассматриваемых задач облегчены применением универсальных алгоритмов обучения нейронных сетей на обучающих выборках.

Если информация о распознаваемых объектах или процессах достаточно полна, то для создания распознающих систем может использоваться значительное число различных нейронных сетей. Однако при разработке систем распознавания динамических процессов реальных технических объектов разработчики сталкиваются с тем, что информация об объекте далека от полноты и будет уточняться в процессе функционирования объекта. Это резко сужает круг сетей-кандидатов, которые целесообразно использовать в подобных распознающих системах, поскольку во многих сетях обучение новому образу, ситуации или ассоциации в общем случае требует полного переобучения сети [1–3]. Невозможность с помощью указанных нейронных сете решить проблему чувствительности (пластичности) к новой информации при сохранении (стабильности) имеющейся информации привели к разработке принципиально новых конфигураций нейронных сетей на основе адаптивной резонансной теории (АРТ) [4–6].

Нейронные сети АРТ относят входное изображение к одному из известных классов, если оно в достаточной степени похоже на прототип этого класса. Если найденный прототип соответствует входному изображению с заданной точностью, то он модифицируется, чтобы стать более похожим на предъявленное изображение. Если входное изображение сети АРТ не похоже в достаточной степени ни на одно из изображений, хранящихся в весах связей нейронной сети, то на его основе создается новый класс. Это возможно благодаря наличию в сети избыточных нейронов, которые не используются до тех пор, пока в этом нет необходимости (если избыточных нейронов нет и входное изображение не относится ни к одному из известных классов, то оно не вызывает реакции сети). Таким образом, нейронные сети АРТ могут запоминать новую информацию без искажения имеющейся информации или переобучения сети.

Непрерывные и дискретные сети адаптивной резонансной теории АРТ-1 и АРТ-2 могут эффективно использоваться при работе систем распознавания в условиях существенной априорной неопределенности, когда необходимо распознавать десятки или сотни различных изображений. Однако использование этих сетей в реальных системах управления, где необходимо распознавать динамические режимы объектов по множеству изменяющихся переменных, затруднено из-за большого разнообразия конкретной измерительной информации об одних и тех же динамических режимах объектов управления (тысячи и даже десятки тысяч различных графических отображений одного и того же режима). Это порождает сложную проблему селекции и хранения существенной

информации [7], поскольку прямое использование сетей АРТ в таких случаях проблематично из-за слишком большого числа необходимых нейронов.

В работах [7, 8] для дискретных сетей АРТ-1 предложена новая архитектура сетей и метод компактного хранения информации, что позволило использовать дискретные нейронные сети АРТ для распознавания различных динамических режимов работы технологического агрегата. Однако применение дискретных сетей АРТ для распознавания режимов функционирования агрегата только по пяти измеряемым переменным требовало использования более пятнадцати тысяч двоичных нейронов. Замена дискретной нейронной сети АРТ на непрерывную сеть АРТ может существенно уменьшить число нейронов в системах распознавания и расширить область применения непрерывных нейронных сетей АРТ.

1. НЕПРЕРЫВНАЯ НЕЙРОННАЯ СЕТЬ АРТ С НОВЫМ НОРМИРОВАНИЕМ ВХОДНЫХ ВЕКТОРОВ

Целью статьи является разработка непрерывных нейронных сетей АРТ для решения задач распознавания режимов функционирования динамических объектов в условиях существенной априорной неопределенности.

Непрерывные нейронные сети АРТ нельзя непосредственно использовать для распознавания режимов функционирования динамических объектов. Это связано с наличием в базовой архитектуре непрерывной нейронной сети АРТ-2 следующих особенностей:

1. Применение в архитектуре сети АРТ-2 нормирования компонент входного вектора $S = (s_1, ..., s_n)$ с помощью соотношения

$$s_i^{\text{н}} = s_i \Big/ \sqrt{\sum_{i=1}^{n} s_i^2}, \quad i = 1, \ldots, n. \tag{1}$$

Такое нормирование позволяет воспринимать любые процессы, одинаковые по форме, но различные по амплитуде как относящиеся к одному классу. Однако при распознавании динамических режимов подобные процессы часто характерны для различных режимов функционирования динамических объектов.

2. В базовой архитектуре сети АРТ-2 отсутствует возможность одновременного сравнения входного изображения с двумя или большим числом изображений, хранящихся в памяти сети. Однако при распознавания режимов функционирования динамических объектов такая возможность необходима.

Для адаптации нейронной сети АРТ-2 к решению задач распознавания режимов функционирования динамических объектов в ее архитектуру и алгоритмы работы внесены следующие изменения:

1. Изменено нормирование компонент входного вектора $S = (s_1, ..., s_n)$:

$$s_i^{\text{н}} = s_i / s_{i\max}, \tag{2}$$

где $s_{i\max}$ – максимально возможное значение i-й (i = 1, ..., n) компоненты для всех допустимых входных векторов нейронной сети.

2. Изменено определение параметра p сходства изображений.

Эти изменения привели к трансформации архитектуры и алгоритмов функционирования нейронной сети АРТ. Новая архитектура сети изображена на рис. 1. Она включает три слоя нейронов: слой входных S-нейронов, сигналы которых нормируются с помощью нормализующего модуля N; слой интерфейсных P-нейронов; слой распознающих Y-нейронов, а также управляющий нейрон R.

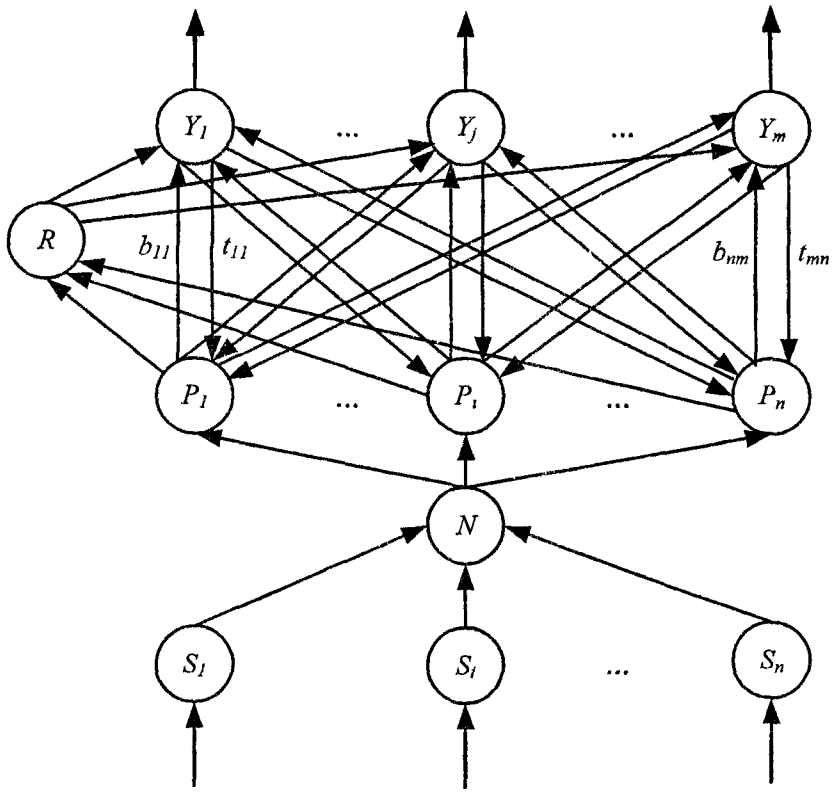

Рис. 1. Новая архитектура нейронной сети АРТ-2

Алгоритм обучения новой непрерывной нейронной сети предполагает выполнение ующих шагов:

Шаг 1. Инициируется параметр p сходства изображений, максимально возможные значения $s_{i\max}$ компонент для входных векторов нейронной сети и веса связей b_{ij} и t_{ji} ($i = 1, \ldots, n; j = 1, \ldots, m$).

Шаг 2. Пока не выполняются условия останова, реализуются шаги 3 – 14 алгоритма.

Шаг 3. Для каждого обучающего входного вектора S^k ($k = 1, \ldots, n$) выполняются шаги 4 – 13 алгоритма.

Шаг 4. Задаются нулевые выходные сигналы для всех элементов Y-слоя: $U_{выхY_j} = 0, j = 1, \ldots, m$. Входным вектором S^k активируются S-элементы входного слоя: $U_{выхS_i} = s_i^k$, $i = 1, \ldots, n$.

Шаг 5 Нормируются выходные сигналы нейронов входного слоя:

$$U_{вхP_i} = \frac{U_{выхS_i}}{U_{выхS_{i\max}}}, \; i = 1, \ldots, n.$$

Шаг 6. Формируются выходные сигналы элементов интерфейсного слоя:

$$U_{выхP_i} = U_{вхP_i}, \; i = 1, \ldots, n.$$

Шаг 7 Для каждого Y-нейрона рассчитывается его выходной сигнал:

$$U_{выхY_j} = U_{вхY_j} = \sum_{i=1}^{n} b_{ij} U_{выхP_i}, \; j = 1, \ldots, m.$$

Шаг 8 Пока не найден Y-нейрон, весовой вектор которого в соответствии с заданным значением параметра сходства p соответствует входному вектору S^*, выполняются шаги 9 – 12 алгоритма.

Шаг 9 В Y-слое определяется нейрон Y_J, удовлетворяющий условию:

$$U_{выхY_J} \geq U_{выхY_j},\ j = 1, \ldots, m.$$

Если таких элементов несколько, то выбирается элемент с наименьшим индексом. Если $U_{выхY_J} = -1$, то все элементы заторможены и входное изображение не может быть классифицировано или сохранено.

Шаг 10. Рассчитываются выходные сигналы элементов интерфейсного слоя:

$$U_{выхP_i} = U_{вхP_i} = U_{выхY_J} t_{Ji},\ i = 1, \ldots, n.$$

Шаг 11 Определяется параметр сходства p_1 для нейрона-победителя.

Шаг 12. Проверяется условие обучения выделенного нейрона Y_J.

Если $p_1 < p$, то условие не выполняется, нейрон Y_J затормаживается ($U_{выхY_J} = -1$) и исключается из дальнейшего участия в соревнованиях при предъявлении данного изображения, затем определяется новый нейрон-победитель (шаг 9 алгоритма). Если $p_1 \geq p$, то условие возможного обучения нейрона Y_J выполняется и осуществляется переход на следующий шаг алгоритма.

Шаг 13. Определяются веса связей элемента Y_J:

$$b_{iJ} = U_{вхP_i},\ t_{Ji} = U_{вхP_i},\ i = 1, \ldots, n.$$

Шаг 14 Проверяются условия останова.

Шаг 15 Останов.

2. НЕЙРОННАЯ СЕТЬ ДЛЯ РАСПОЗНАВАНИЯ ПРОЦЕССОВ ПО ИХ ПРИНАДЛЕЖНОСТИ К ОПРЕДЕЛЕННЫМ ОБЛАСТЯМ ИЗМЕНЕНИЯ ПЕРЕМЕННЫХ

Для распознавания по принадлежности к определенным областям D_k^l $(l = 1, \ldots, L;\ k = 1, \ldots, K)$ изменения переменных $I_k(t_i)$ заданного числа L режимов функционирования объекта необходимо сформировать эти области на основе обучающих процессов (изображений). В базовой структуре нейронной сети АРТ-2 отсутствует механизм формирования таких областей. В связи с этим на стадии предварительной обработки информации предлагается для каждой переменной $I_k(t_i)$ в любом из L режимов функционирования объекта определять по две функции (изображения):

$$I_{k\min}^l(t_i) = \min(I_{k1}^l(t_i), I_{k2}^l(t_i), \ldots, I_{knl}^l(t_i)),\ l = 1, \ldots, L,\ k = 1, \ldots, K, t_i = 0, 1, 2, \ldots, \quad (3)$$

$$I_{k\max}^l(t_i) = \max(I_{k1}^l(t_i), I_{k2}^l(t_i), \ldots, I_{knl}^l(t_i)),\ l = 1, \ldots, L,\ k = 1, \ldots, K, t_i = 0, 1, 2, \ldots, \quad (4)$$

где $I_{k\min}^l(t_i)$, $I_{k\max}^l(t_i)$ – минимальное и максимальное значение переменной $I_k(t_i)$ $(k = 1, \ldots, K)$ в l-м режиме функционирования объекта в учитываемом множестве $I_{k1}^l(t_i), I_{k2}^l(t_i), \ldots, I_{knl}^l(t_i)$ обучающих процессов в момент времени t_i; n_l – число учитываемых изображений при обучении сети распознаванию l-го динамического режима.

Затем все $2LK$ функций (3), (4) используются для обучения новой непрерывной нейронной сети АРТ.

Для определения принадлежности входного изображения $I_k(t_i)$, $(k=1,...,K)$ некоторому l-му режиму функционирования объекта необходимо выполнить его сравнение с двумя изображениями $I^l_{k\min}(t_i)$ и $I^l_{k\max}(t_i)$. При этом сравнение выполняется с определением значения параметра сходства p. В базовой архитектуре непрерывной нейронной сети АРТ-2 отсутствует возможность одновременного сравнения с двумя изображениями. Поэтому предлагается новая сеть адаптивной резонансной теории АРТ-2Д – непрерывная сеть для распознавания динамических режимов. Сеть состоит из двух параллельно работающих модулей, каждый из которых является модифицированной сетью АРТ-2. Первый модуль (рис. 2) предназначен для запоминания в режиме обучения соотношений (3), а второй – соотношений (4). В режиме распознавания первый модуль выполняет сравнение входного изображения с функциями, описываемыми выражениями (3), а второй модуль – соответственно с функциями, описываемыми выражениями (4). При задании L режимов функционирования объекта по переменным $I_k(t_i)$ $(k=1,...,K)$ с помощью соотношений (3), (4) нетрудно представить ситуацию, когда по $I^l_{k\min}(t_i)$ или по $I^l_{k\max}(t_i)$ выполняется соответственно L соотношений:

$$I_k(t_i) \geq I^l_{k\min}(t_i), \quad l=1,...,L$$

или

$$I_k(t_i) \leq I^l_{k\max}(t_i), \quad l=1,...,L.$$

В связи с этим введены связи между парами Y^1_i и Y^2_i $(i=1,...,m)$ Y-нейронов, предназначенных для распознавания одного и того же режима функционирования объекта в разных модулях. С помощью этих связей Y-нейроны первого модуля управляют соответствующими распознающими нейронами второго модуля.

Нейрон-победитель второго модуля выделяется не в результате соревнования между распознающими элементами, а сигналом с нейрона-победителя Y^1_J первого модуля после проверки соответствия нейрона Y^1_J по величине параметра сходства p входного изображения и изображения, хранящегося в весах его связей. Выделенный нейрон Y^2_J второго модуля также проверяется по величине параметра сходства p. Если он выдерживает эту проверку и выдерживает последующую проверку по величине параметра сходства и пара нейронов Y^1_J и Y^2_J, то на выходе распознающего нейрона Y_J сети АРТ-2Д появляется единичный сигнал, свидетельствующий о распознавании наблюдаемого режима функционирования объекта. Если нейрон Y^2_J или пара элементов Y^1_J, Y^2_J не выдерживают проверку по величине параметра сходства, то нейрон Y^1_J затормаживается $(U_{вых Y^1_J} = -1)$, а нейрон Y^2_J переводится в неактивное состояние $(U_{вых Y^2_J} = 0)$.

Отметим, что непосредственно выполнить проверку пары элементов Y^1_J, Y^2_J по величине параметра сходства p при известных параметрах сходства p_1 и p_2 соответственно для нейронов Y^1_J и Y^2_J нельзя. Ее необходимо осуществлять с помощью параметров несходства:

$$p^{\text{н}} = 1-p, \quad p_1^{\text{н}} = 1-p_1, \quad p_2^{\text{н}} = 1-p_2, \qquad (5)$$

где $p^{н}$ – параметр несходства входного изображения с изображениями, хранящимися в весах связей нейронов Y_J^1 и Y_J^2; $p_1^{н}, p_1$ – соответственно параметр несходства и параметр сходства входного изображения с изображениями, хранящимися в весах связей нейрона Y_J^1; $p_2^{н}, p_2$ – соответственно параметр несходства и параметр сходства входного изображения с изображениями, хранящимися в весах связей нейрона Y_J^2.

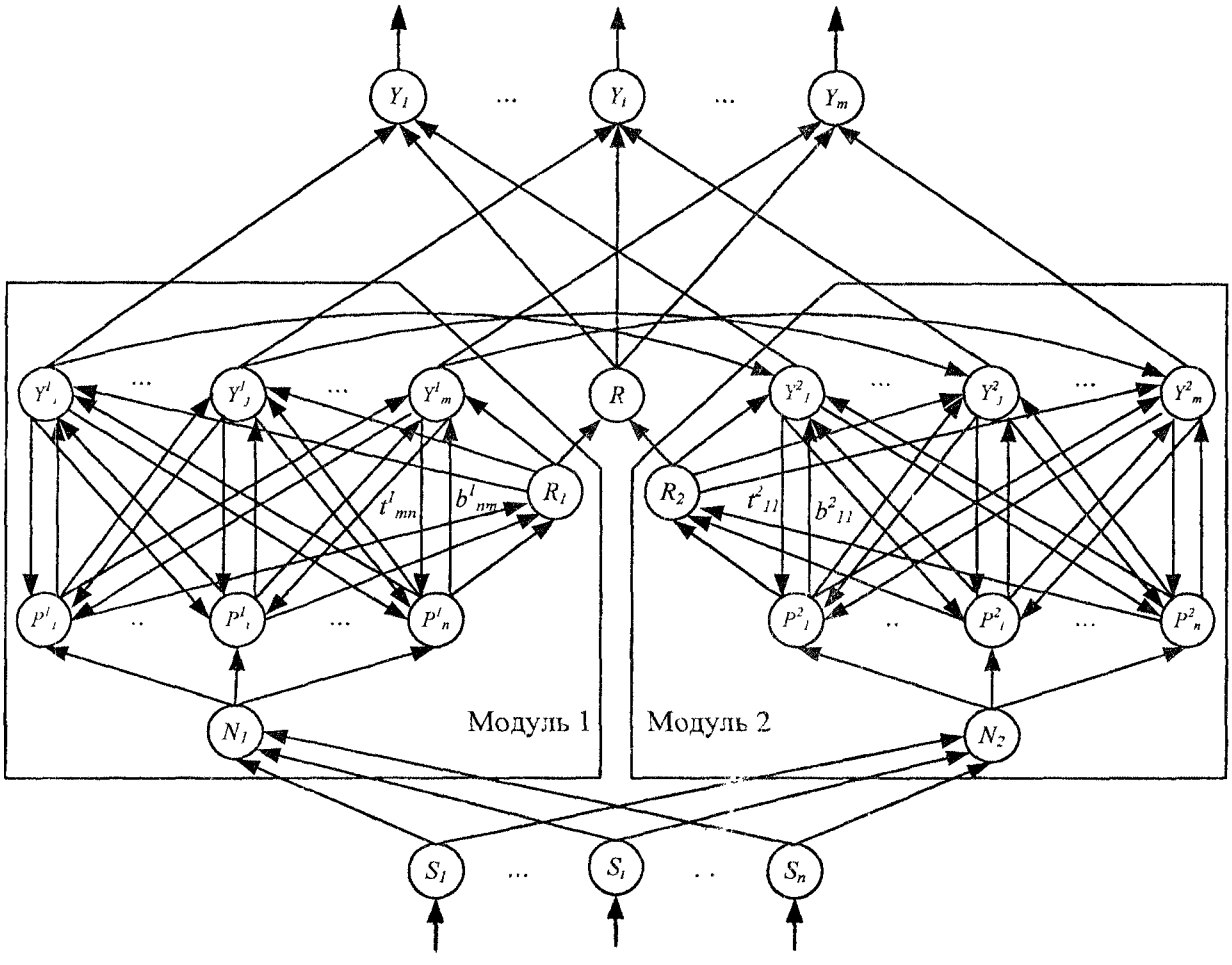

Рис. 2. Архитектура нейронной сети АРТ-2Д

Параметры несходства $p_1^{н}, p_2^{н}$ показывают соответственно относительное число компонент входного изображения, которые не удовлетворяют ограничениям (3) или (4), а их сумма $p_1^{н} + p_2^{н}$ – общее число компонент входного изображения, не соответствующих образу, хранящемуся в весах связей нейронов Y_J^1 и Y_J^2. Очевидно, что для изображений данного образа должно выполняться условие

$$p_1^{н} + p_2^{н} \le p^{н}. \qquad (6)$$

Используя соотношения (5), из выражения (6) нетрудно получить новое неравенство, с помощью которого можно проверять, удовлетворяет ли пара нейронов Y_J^1 и Y_J^2 по значению параметра сходства p, если известны параметры сходства для каждого из отдельных нейронов:

$$p_1 + p_2 - 1 \ge p.$$

Алгоритм функционирования сети АРТ-2Д при распознавании динамических режимов предусматривает выполнение следующих шагов:

Шаг 1. Инициализация параметров.

Шаг 2. Для распознаваемого входного вектора $S = (s_1, ..., s_n)$ выполняются шаги 3–15 алгоритма.

Шаг 3. Задаются для двух модулей нейронной сети нулевые выходные сигналы всех распознающих элементов Y_J^1- и Y_J^2-слоя:

$$U_{выхY_j^1} = 0,\ U_{выхY_j^2} = 0,\ j = 1, \ldots, m.$$

Распознаваемым вектором S активируются S-элементы входного слоя:

$$U_{выхS_i} = s_i,\ i = 1, \ldots, n.$$

Шаг 4. Нормируются выходные сигналы нейронов входного слоя:

$$U_{вхP_i^1} = U_{выхN_1} = U_{выхS_i} / U_{выхS_i\max},\ i = 1, \ldots, n.$$

Шаг 5. В первом модуле нейронной сети определяются выходные сигналы элементов интерфейсного слоя:

$$U_{выхP_i^1} = U_{вхP_i^1},\ i = 1, \ldots, n.$$

Шаг 6. Рассчитываются выходные сигналы распознающих нейронов:

$$U_{выхY_j^1} = \sum_{i=1}^{n} b_{ij}^1 U_{выхP_i^1},\ j = 1, \ldots, m.$$

Шаг 7. Пока не найден Y_J^1– нейрон-победитель первого модуля нейронной сети, выполняется шаг 8 алгоритма.

Шаг 8. В Y^1 – слое первого модуля нейронной сети определяется нейрон Y_J^1, удовлетворяющий условию

$$U_{выхY_J^1} \geq U_{выхY_j^1},\ j = 1, \ldots, m.$$

Если таких элементов несколько, то выбирается элемент с наименьшим индексом. Если $U_{выхY_J^1} = -1$, то все элементы заторможены и входное изображение не может быть правильно классифицировано (переход к шагу 15 алгоритма).

Шаг 9. Определяется значение параметра сходства p_1 для нейрона-победителя Y_J^1 по соотношению:

$$p_1 = \frac{\left\| P_1^{l*}(k, t_i) \right\|}{K(T+1)},$$

где $P_1^{l*}(k, t_i)$ – функция, соответствующая l-му динамическому режиму, распознаваемому по минимальным значениям $I_{k\min}^l(t_i)$ динамических процессов $I_k^l(t_i)$;

Норма функции $P_1^{l*}(k, t_i)$ определяется соотношением:

$$\left\| P_1^{l*}(k, t_i) \right\| = \sum_{k=1}^{K} \sum_{t_i=0}^{T} P_1^{l*}(k, t_i).$$

$$P_1^{l*}(k, t_i) = \begin{cases} 1, \text{если } I_{k\min}^l(t_i) \leq I_k^{l*}(t_i),\ k = 1, ..., K, t_i = 0, 1, ..., T, \\ 0, \text{если } I_{k\min}^l(t_i) > I_k^{l*}(t_i),\ k = 1, ..., K,\ t_i = 0, 1, ..., T. \end{cases}$$

Шаг 10. Проверяется соответствие параметра сходства: $p_1 \geq p$, где p – параметр сходства входного изображения и изображения, хранящегося в весах связей нейрона-победителя Y_J^1 первого модуля. Если условие не выполняется, то нейрон Y_J^1 затормаживается и исключается из дальнейшего участия в соревнованиях при предъявлении данного изображения, затем определяется новый нейрон-победитель первого модуля (шаг 8 алгоритма). Если условие выполняется, то возможен переход на следующий шаг алгоритма.

Шаг 11. Нейрон Y_J^1 первого модуля своим выходным сигналом на вход нейрона Y_J^2 второго модуля превращает его в нейрон-победитель второго модуля.

Шаг 12. Определяются параметр сходства p_2 и параметр несходства $p_2^{\text{н}}$ для входного изображения и изображения, хранящегося в весах связей нейрона-победителя Y_J^2 второго модуля:

$$p_2 = \frac{\left\| P_2^{l*}(k,t_l) \right\|}{K(T+1)}, \quad p_2^{\text{н}} = 1 - p_2,$$

где $P_2^{l*}(k,t_l)$ – функция, соответствующая l-му динамическому режиму, распознаваемому по максимальным значениям $I_{k\max}^l(t_l)$ динамических процессов $I_k^l(t_l)$;

$$P_2^{l*}(k,t_l) = \begin{cases} 1, \text{если } I_{k\max}^l(t_l) \geq I_k^{l*}(t_l), \quad k = 1,...,K, \quad t_l = 0,1,...,T, \\ 0, \text{если } I_k^{l*}(t_l) < I_{k\max}^l(t_l), \quad k = 1,...,K, \quad t_l = 0,1,...,T, \end{cases}$$

где $\left\| P_2^{l*}(k,t_l) \right\|$ – норма функции $P_2^{l*}(k,t_l)$, определяется соотношением:

$$\left\| P_2^{l*}(k,t_l) \right\| = \sum_{k=1}^{K} \sum_{t_l=0}^{T} P_1^{l*}(k,t_l).$$

Шаг 13. Проверяется соответствие по значению параметра сходства входных процессов, по верхним границам областей D_k^l $(k = 1,...,K)$ l-го режима функционирования динамического объекта: $p_2 \geq p$. Если условие не выполняется, то нейроны Y_J^1, Y_J^2 обоих модулей сети исключаются из дальнейшего участия в соревнованиях при предъявлении данного входного изображения, затем осуществляется переход к 8-му шагу алгоритма. Если условие выполняется, то возможен переход к следующему шагу алгоритма.

Шаг 14. По вычисленным значениям параметров сходства для обоих модулей сети проверяется соответствие входных процессов $I_k(t_l)$, $k = 1,...,K$, $t_l = 0,1,...,T$ областям D_k^l $(k = 1,...,K)$ l-го режима функционирования динамического объекта:

$$p \leq p_1 + p_2 - 1.$$

Если условие выполняется, то по входным процессам $I_k(t_l)$, $k = 1,...,K$, $t_l = 0,1,...,T$ распознается l-й режим функционирования объекта. Если условие не выполняется, то осуществляется переход к шагу 8 алгоритма и поиск другого режима функционирования объекта, более соответствующего входным процессам.

Шаг 15. Останов.

Математическое моделирование архитектуры и алгоритмов функционирования нейронной сети АРТ-2Д при распознавании различных режимов функционирования динамических объектов подтвердили работоспособность предложенной непрерывной сети адаптивной резонансной теории.

ЗАКЛЮЧЕНИЕ

Разработана новая непрерывная сеть адаптивной резонансной теории АРТ-2Д, позволяющая запоминать и распознавать режимы функционирования реальных динамических объектов. Новая сеть существенно расширяет возможности разработки эффективных систем распознавания на основе сетей адаптивной резонансной теории. В дальнейшем предполагается разработка непрерывных нейронных сетей АРТ с несколькими параллельно работающими полями входных нейронов в каждом из модулей сети. Такие нейронные сети необходимы для распознавания режимов функционирования динамических объектов с большим числом наблюдаемых переменных.

Библиографический список

1. Оссовский, С. Нейронные сети для обработки информации [Текст] / С. Оссовский. – М. : Финансы и статистика, 2002. – 344 с.
2. Руденко, О. Г. Основы теории искусственных нейронных сетей [Текст] / О. Г. Руденко, Е. В. Бодянский. – Харьков : ТЕЛЕТЕХ, 2002. – 317 с.
3. Круглов, В В. Искусственные нейронные сети : теория и практика [Текст] / В. В. Круглов, В. В. Борисов. –М. : Горячая линия – Телеком, 2001. – 382 с.
4. Carpenter, G. A. Massively parallel architecture for self-organizing neural pattern recognition machine [Text] / G. A. Carpenter, S. A. Grossberg // Computing, Vision, Graphics and Image Processing. – 1987. – Vol. 37. – P. 54-115.
5. Grossberg, S. Competitive learning : from interactive activation to adaptive resonance [Text] / S. Grossberg // Cognitive Science. – 1987. – Vol. 11. – P. 23-63.
6. Fausett, L. Fundamentals of Neural Networks: architectures, algorithms and applications [Text] / L. Fausett. – New Jersey : Prentice Hall Int., Inc., 1994. – 461 p.
7. Дмитриенко, В. Д. Специализированное вычислительное устройство для распознавания динамических режимов объектов управления [Текст] / В. Д. Дмитриенко, Р. Д. Расрас, А. М. Сырой // Інформаційно-керуючі системи на залізничному транспорті. – 2002. – № 1. – С. 15-22.
8. Дмитриенко, В. Д. Повышение точности и стабильности информационно-измерительных систем на основе нейронных сетей АРТ [Текст] / В. Д. Дмитриенко, Р. Д. Расрас // Вестник ХГПУ. – 2000. – Вып. 92. – С. 149-154.

УДК 621.391

СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ НА АЛГЕБРАИЧЕСКИХ БЛОКОВЫХ КОДАХ

А. А. Кузнецов

ВВЕДЕНИЕ

Симметричные криптосистемы на алгебраических блоковых кодах (теоретико-кодовые схемы) впервые предложены в работе Рао и Нама [1]. Основная идея, заложенная в эту конструкцию, состоит в использовании в качестве секретного ключа порождающей матрицы G линейного блокового (n, k, d) кода. Шифрованная информация (криптограмма) в виде вектора c^* длины n формируется по правилу

$$c^* = I \cdot G + e, \qquad (1)$$

где вектор $c = I \cdot G$ принадлежит (n, k, d) коду с порождающей матрицей G, I – k-разрядный информационный вектор, вектор e – секретный (случайный) вектор ошибок.