УДК 004.032.26, 004.94, 004.056.5 DOI: 10.17587/it.24.351-359

А. А. Коляда, д-р физ.-мат. наук, доц., гл. науч. сотр., **П. В. Кучинский,** д-р физ.-мат. наук, проф.,
Научно-исследовательское учреждение "Институт прикладных физических проблем
имени А. Н. Севченко" Белорусского государственного университета, Минск, Беларусь,
Н. И. Червяков, д-р техн. наук, проф., e-mail: razan@tut.by, niipfp@bsu.by, Chervyakov@yandex.ru,
Северо-Кавказский федеральный университет, Ставрополь, РФ

Редукционный метод позиционно-модулярного преобразования больших чисел для нейронных сетей на конечных кольцах

Рассматривается проблема построения нейронных сетей конечного кольца (НСКК), которые служат основой нейросетевых модулярных вычислительных структур для высокопроизводительных криптографических приложений. Методологическую базу НСКК исследуемого класса составляет модифицированный редукционный метод позиционно-модулярного преобразования взвешенных больших чисел. Дана математическая формализация метода, получены оценки диапазона изменения и разрядности элементов последовательности вычетов, формируемой по применяемой редукционной схеме рекурсивного типа, исследованы характер и скорость ее сходимости, предложен гибкий табличный механизм сокращения числа итераций схемы. Синтезирован общий редукционный алгоритм позиционно-модулярного кодового преобразования, разработана параллельная структура НСКК, осуществляющей базовое преобразование за одну итерацию.

Ключевые слова: *нейронная сеть, нейронная сеть конечного кольца, синаптические веса, модулярная система счисления, модулярная арифметика, криптография, диапазон больших чисел, редукционный метод позиционно-модулярного преобразования*

Введение

В современном процессе развития эффективных средств защиты информации фундаментальная роль отводится разработкам по созданию новых вычислительных технологий, ориентированных на высокоскоростную реализацию трудоемких базовых процедур в диапазонах больших чисел (ДБЧ) [1—8]. С точки зрения производительности при оперировании на ДБЧ приоритетные позиции принадлежат модулярным вычислительным технологиям. Важнейшим фактором, способствующим неуклонному повышению уровня востребованности данных технологий, является их идеальная приспособленность к нейросетевым реализациям [1, 3, 9—13]. Активно развиваемое в настоящее время новое направление в криптографии — разработка и оптимизация нейросетевых модулярных вычислительных структур (МВС) [1, 3], нацеленное на реализацию в максимальной мере оптимально согласованных свойств параллелизма искусственных нейронных сетей (ИНС) и модулярной арифметики (МА), дает принципиально новые возможности для построения высокопроизводительных криптосистем различного функционального назначения. Отмеченное обстоятельство обусловлено тем, что при согласованном числе синапсов нейронной сети (НС), используемых в процессе взаимодействия ее нейронов, и мощностью базиса применяемой модулярной системы счисления (МСС) НС становится естественным представлением данной числовой системы [12]. На адекватность системы счисления в остатках и НС указывают, в частности, следующие признаки:

- семантическое сходство позиционных форм модулярных чисел с расчетными соотношениями формального нейрона;
- существование адекватного отображения алгоритмов арифметических операций в МСС на многослойные НС;
- простота реализации основных операций нейросетевого логического базиса в модулярном коде;
- равнозначность модулярного кодирования информации и ассоциативной нейронной па-

мяти, вытекающая из смыслового (семантического) соответствия оснований МСС классификационному признаку сети, а остаткам по основаниям — значению этого признака.

Основополагающая идея теоретических и прикладных разработок по созданию методологических, алгоритмических и программно-аппаратных средств реализации позиционных форм модулярных чисел [1, 2, 14, 15] состоит в переводе вычислений из ДБЧ в компьютерные диапазоны целых чисел (ЦЧ) стандартной разрядности. Ключевую роль в процессе решения сформулированной задачи выполняют НС, определенные на конечных кольцах вычетов по рабочему базису модулей. Операционную основу нейронных сетей конечного кольца (НСКК) составляют главным образом операции приведения целых чисел к остаткам по используемым модулям. Как структурно, так и на операционном уровне НСКК в максимальной мере должны быть согласованы с естественным кодовым параллелизмом МА. В полной мере данному условию удовлетворяет рассматриваемый в настоящей работе редукционный метод позиционно-модулярного кодового преобразования.

1. Математическая формализация редукционного метода позиционно-модулярного преобразования больших чисел

Введем обозначения:

- $\mathbf{Z}$ — множество целых чисел;
- $\lfloor a \rfloor$ и $\lceil a \rceil$ — наибольшее и наименьшее ЦЧ соответственно, не большее и не меньшее вещественной величины a;
- $\mathbf{Z}_m = \{0, 1, ..., m-1\}$, $\mathbf{Z}^-_m = \{-\lfloor m/2 \rfloor, -\lfloor m/2 \rfloor + 1, ..., \lceil m/2 \rceil - 1\}$ — множества наименьших неотрицательных и абсолютно наименьших вычетов по натуральному модулю m;
- $|a|_m$ и $|a|^-_m$ — элементы множеств $\mathbf{Z}_m$ и $\mathbf{Z}^-_m$, сравнимые с a (в общем случае рациональным числом) по модулю m.

Функциональное назначение НС конечного кольца по модулю m исследуемого класса состоит в вычислении остатка от деления произведения CX на m,

$$\chi = |CX|_m, \tag{1}$$

где C — целочисленная константа; X — входное неотрицательное ЦЧ, представленное b-разрядным двоичным кодом $(x_{b-1}\ x_{b-2} \dots\ x_0)_2$ ($x_j \in \{0,1\}$, $j = \overline{0, b-1}$. По критерию простоты нейросетевой реализации наиболее приемлемым методом выполнения операции (1) является метод модулярной редукции суммы взвешенных операндов по рекурсивной схеме последовательного снижения разрядности получаемых вычетов [1, 3].

Положим

$$\begin{aligned} X^{(0)} &= (x^{(0)}_{b_0-1}\ x^{(0)}_{b_0-2} \dots\ x^{(0)}_0)_2 = \\ &= \sum_{j=0}^{b_0-1} 2^j x^0_j \ (b_0 = b,\ x^{(0)}_j = x_j) \end{aligned} \tag{2}$$

и пусть

$$W_j(C) = \left|C \cdot 2^j\right|^-_{m_0} = \begin{cases} \left|C \cdot 2^j\right|_m, \text{ если } \left|C \cdot 2^j\right|_m < \left\lceil \dfrac{m}{2} \right\rceil, \\ \left|C \cdot 2^j\right|_m - m, \text{ если } \left|C \cdot 2^j\right|_m \geqslant \left\lceil \dfrac{m}{2} \right\rceil, \end{cases} \quad j = \overline{0, b-1}. \tag{3}$$

При $C = 1$ далее используется обозначение $W_j = W_j$ (1).

Применяемая редукционная схема описывается операционной последовательностью:

$$\begin{aligned} &\Big\langle X^{(1)} = \sum_{j=0}^{b_0-1} W_j(C)\, x^{(0)}_j = \\ &= (x^{(1)}_{b_1-1} x^{(1)}_{b_1-2} \dots x^{(1)}_0)_2 - 2^{b_1} x^{(1)}_{b_1-1} = \\ &= \sum_{j=0}^{b_1-2} 2^j x^{(1)}_j - 2^{b_1-1} x^{(1)}_{b_1-1}, \\ &X^{(s)} = \sum_{j=0}^{b_{s-1}-2} W_j x^{(s-1)}_j - W_{b_{s-1}-1} x^{(s-1)}_{b_{s-1}-1} = \\ &= (x^{(s)}_{b_s-1}\ x^{(s)}_{b_s-2} \dots x^{(s)}_0)_2 - 2^{b_s} x^{(s)}_{b_s-1} = \\ &= \sum_{j=0}^{b_s-2} 2^j x^{(s)}_j - 2^{b_s-1} x^{(s)}_{b_s-1} \ \left(s = \overline{2, S}\right); \Big\rangle, \\ &\chi = \left|X^{(S)}\right|_m, \end{aligned} \tag{4}$$

где b_1 и b_s — длины дополнительных двоичных кодов $(x^{(1)}_{b_1-1} x^{(1)}_{b_1-2} \dots x^{(1)}_0)_2$ и $(x^{(s)}_{b_s-1} x^{(s)}_{b_s-2} \dots x^{(s)}_0)_2$ соответственно ЦЧ $X^{(1)}$ и $X^{(s)}$, которые, как следует из (4), в принципе могут быть и отрицательными; S — число итераций схемы.

В целях получения необходимой информационной базы для исследования характера скорости сходимости и оптимизации числа S итераций рекурсивного процесса (4) — преобразований типа $X \to |CX|_m$, оценим мощность диапазона изменения ЦЧ $X^{(s)}$ и его разрядность b_s.

Предположим, что m — простое число и обозначим его разрядность через $b\_\mathrm{mod} = [\log_2 m]$ бит.

Как известно [16, 17], множество всех степеней числа 2 по модулю m в мультипликативной группе кольца $\mathbf{Z}_m$ образуют так называемую циклическую подгруппу, порождаемую элементом 2. Порядок N этой подгруппы (число ее элементов) служит делителем функции Эйлера $\varphi(m) = m - 1$. Сказанное относится и к совокупности абсолютно наименьших остатков от деления указанных степеней на m, т. е. к определяемому по формуле (3) набору вычетов:

$$\{W_j \in \mathbf{Z}_m^- | W_j = \left|2^j\right|_m^-; j = \overline{0, N-1}\}. \qquad (5)$$

При $b\_\mathrm{mod} < b_{s-1}$ последовательности весовых коэффициентов

$$\{W_0,\ W_1,\ ...,\ W_{N-1},\ W_N,\ ...,\ W_{b_{s-1}-1}\}\ (s = \overline{2,S}), \qquad (6)$$

используемые в (4), имеют циклическую структуру. Сегменты длины N в (6) с начальными элементами $W_{iN}\left(i = 0, \overline{b_{s-1}/N - 1}\right)$ совпадают с последовательностью (5). В случае, когда b_{s-1} не делится нацело на N, последний $[b_{s-1}/N]$-й сегмент в (6) оказывается неполным. Пусть N_+ и N_- — количества соответственно положительных и отрицательных вычетов в множестве (5). Тогда с учетом вышеизложенного при $s = \overline{2,S}$ максимально возможное значение числа $X^{(s)}$ (см. (4)) сверху можно оценить следующим образом:

$$\max\left\{X^{(s)}\right\} < \frac{b_{s-1}}{N}\sum_{j=0}^{N_+-1}\left(\frac{m-1}{2} - 1\right) =$$
$$= \frac{b_{s-1}}{N}\left(\frac{m-1}{2} + \frac{m-1}{2} - N_+ + 1\right)\frac{N_+}{2} =$$
$$= \frac{b_{s-1}}{N}(m - N_+)\frac{N_+}{2}.$$

Аналогично для минимального значения ЦЧ $X^{(s)}$ верна следующая оценка:

$$\min\left\{X^{(s)}\right\} > \frac{b_{s-1}}{N}\sum_{j=0}^{N_--1}\left(-\frac{m-1}{2} + j\right) =$$
$$= \frac{b_{s-1}}{N}\left(-\frac{m-1}{2} - \frac{m-1}{2} + N_- - 1\right)\frac{N_-}{2} =$$
$$= -\frac{b_{s-1}}{N}(m - N_-)\frac{N_-}{2}.$$

Следовательно,

$$\max\left\{X^{(s)}\right\} - \min\left\{X^{(s)}\right\} <$$
$$< \frac{b_{s-1}}{N}\left(\frac{N_+}{2}(m - N_+) + \frac{N_-}{2}(m - N_-)\right) =$$
$$= \frac{b_{s-1}}{N}\left(\frac{m}{2}(N_+ + N_-) - \frac{N_+^2 + N_-^2}{2}\right) =$$
$$= \frac{b_{s-1}}{2N}\left(mN - \left(N_+^2 + N_-^2 + 2N_+N_- - 2N_+N_-\right)\right) =$$
$$= \frac{1}{2}b_{s-1}\left(m - \frac{(N_+ + N_-)^2}{N} + \frac{2N_+N_-}{N}\right) =$$
$$= \frac{1}{2}b_{s-1}\left(m - N + 2N\left(\left(\frac{N_+}{N}\frac{N_-}{N}\right)^{\frac{1}{2}}\right)^2\right) \leqslant \qquad (7)$$
$$\leqslant \frac{1}{2}b_{s-1}\left(m - N + 2N\left(\frac{N_+}{N} + \frac{N_-}{N}\right)\frac{1}{4}\right) =$$
$$= \frac{1}{2}b_{s-1}\left(m - N + \frac{1}{2}N\right) = \frac{1}{2}b_{s-1}\left(m - \frac{1}{2}N\right).$$

Так как N является делителем функции Эйлера $\varphi(m) = m - 1$, то N представимо в виде $N = (m-1)/d$, где d — делитель ЦЧ $\varphi(m) = m - 1$ ($d \neq N$). С учетом отмеченного обстоятельства из выражения (7) получаем

$$\max\{X^{(s)}\} - \min\left\{X^{(s)}\right\} < \frac{1}{2}b_{s-1}\left(m - \frac{m-1}{2d}\right) =$$
$$= \frac{1}{2}b_{s-1}m\left(1 - \frac{1}{2d} + \frac{1}{2dm}\right).$$

Отсюда заключаем, что

$$\log_2\left(\max\{X^{(s)}\} - \min\{X^{(s)}\} + 1\right) + 1 <$$
$$< \log_2(b_{s-1}) + b\_\mathrm{mod} + \log_2\left(1 - \frac{1}{2d} + \frac{1}{2dm}\right).$$

Таким образом, ввиду того, что $1/2 < 1 - 1/(2d) + 1/(2dm) < 1$ для разрядности ЦЧ $X^{(s)}$ справедлива оценка:

$$b_s = \lceil \log_2(\max\{X^{(s)}\} - \min\{X^{(s)}\} + 1) \rceil <$$
$$< b\_\mathrm{mod} + \log_2(b_{s-1}). \qquad (8)$$

Что касается числа $X^{(1)}$ (см. (4)), то для оценки его разрядности b_1 также применим рассмотренный выше подход. Это обеспечивается тем, что при любом целочисленном C последовательность $\{W_0(C),\ W_1(C),\ ...,\ W_{N-1}(C),\ W_N(C),\ W_{N+1}(C),\ ...,\ W_{2N-1}(C),\ ...,\ W_{b_0-1}(C)\}$ абсолютно наименьших остатков по модулю m, определяемых по правилу (3), благодаря выполнению равенств $W_{iN+j}(C) = W_j(C)$ $\left(i = \overline{1, \left\lfloor \frac{b_0}{N} \right\rfloor - 1};\ j = \overline{0, N-1}\right)$, как и последовательности (6), имеет циклическую структуру (с пе-

риодом N). Математические выкладки, приведенные выше для $X^{(s)}$ ($s = \overline{2,S}$), дают для разрядности b_1 числа $X^{(1)}$ оценку аналогичную (8), а именно оценку вида:

$$b_1 < b\_\mathrm{mod} + \log_2 b_0 = b\_\mathrm{mod} + \log_2 b. \qquad (9)$$

Несмотря на то что оценочные значения (8), (9) разрядностей b_s ($s = \overline{1,S}$) чисел (4) сильно завышены, они вполне адекватно отражают характер сходимости рассматриваемой редукционной схемы.

Рекурсивный редукционный процесс, базирующийся на (2)—(4), обладает следующими свойствами.

А. Числа $X^{(0)} = X$, $|X^{(1)}|$, $|X^{(2)}|$, ..., $|X^{(S)}|$ образуют убывающую последовательность. При этом ввиду (3) все $X^{(s)}$ ($s = \overline{0,S}$) равноостаточны по модулю m, т. е. являются элементами одного и того же класса $\overline{X}$ вычетов по данному модулю: $\overline{X} = \{A \in \mathbf{Z} \,|\, A \equiv X (\mathrm{mod}\, m)\}$ ($\mathbf{Z}$ — множество целых чисел).

Б. Согласно (8), (9) достигаемое на s-й итерации отклонение $\Delta_s = b_s - b\_\mathrm{mod}$ разрядности ЦЧ $X^{(s)}$ от разрядности модуля m составляет порядка $[\log_2 b_{s-1}]$ бит. Поскольку с увеличением s скорость приближения b_s к b_mod снижается, то в целях уменьшения числа S итераций вычислительной схемы (4), а значит и временных затрат на ее реализацию, в качестве признака завершения редукционного процесса принимается выполнение неравенства

$$\Delta_s = b_s - b\_\mathrm{mod} \leqslant \Delta_{\min}, \qquad (10)$$

где $\Delta_{\min}$ — некоторый порог, подбираемый экспериментально (в ходе обучения соответствующей нейронной сети). В частности, при использовании в (10) $\Delta_{\min} = 0$ искомое значение выходной величины схемы (4) формируется по правилу:

$$\chi = \begin{cases} X^{(S)} + m, \text{ если } X^{(S)} < 0, \\ X^{(S)}, \text{ если } 0 \leqslant X^{(S)} < m, \\ X^{(S)} - m, \text{ если } m \leqslant X^{(S)}. \end{cases} \qquad (11)$$

Число S итераций редукционной схемы (4) не превышает оценочного значения, определяемого условием

$$b_s - b\_\mathrm{mod} < \log_2(b\_\mathrm{mod} + \log_2(b\_\mathrm{mod} + \\ + \log_2(...\log_2(b\_\mathrm{mod} + \log_2 b_0) ...))) \leqslant \Delta_{\min} (b_0 = b),$$

которое вытекает из (8)—(10).

В. Расчетные соотношения схемы (4) целиком согласуются с принципами нейросетевой вычислительной технологии. Осуществляя суммирование синаптических весов (3) с последующим вычислением активационной функции $\chi = |CX|_m = |X^{(s)}|_m$, реализуемой, например, в виде (11). Набор необходимых весовых коэффициентов (3) рассчитывается предварительно и хранится в памяти.

Г. Редукционная схема (4) без существенных структурно-функциональных изменений применима для любого числа модулей. Это и обеспечивает возможность совместного использования ИНС и МА.

Д. Метод модулярной редукции для преобразования $X \to |CX|_m$ по рекурсивной вычислительной схеме (4) легко может быть обобщен на случай использования произвольной позиционной системы счисления с основанием $r > 2$ и, в частности, десятичной системы счисления.

2. Редукционный алгоритм позиционно-модулярного кодового преобразования целых чисел

На базе представленного метода последовательного уменьшения разрядности ЦЧ по редукционной схеме (4) рекурсивного типа синтезирован алгоритм позиционно-модулярного кодового преобразования, ориентированный на нейросетевую реализацию, который заключается в нижеследующем.

Параметры алгоритма:

- попарно простые модули $m_1, m_2, ..., m_k$, имеющие соответственно разрядности b_mod_1, b_mod_2, ..., b_mod_k бит ($b\_\mathrm{mod}\_i = [\log_2 m_i]$ ($i = \overline{1,k}$); $k \geqslant 1$);
- порог $\Delta_{\min}$ ($\Delta_{\min} = 0$) для решающего правила (10) завершения редукционного процесса.

Входные данные алгоритма:

- двоичный код $(x_{b-1}\, x_{b-2} \ldots x_0)_2$ исходного ЦЧ X (b — длина кода);
- целочисленные коэффициенты C_i произведений $C_i X$, подлежащих приведению к остаткам по модулям m_i ($i = \overline{1,k}$).

Выходные данные: набор остатков — модулярный код ($\chi_1, \chi_2, ..., \chi_k$) ($\chi_i = \left|C_i X\right|_{m_i}$, $i = \overline{1,k}$) по заданному базису модулей — $\mathbf{M} = \{m_1, m_2, ..., m_k\}$.

Предварительно получаемые данные: рассчитанные согласно правилу (3) наборы весов

$$\mathbf{W}_i(C) = \\ = \left\{ W_{j,i}(C) \,|\, W_{j,i}(C) = \left| C_i 2^j \right|_{m_i}^{-}; j = \overline{0, b-1} \right\}, \qquad (12)$$

$$\mathbf{W}_i = \left\{ W_{j,i} \,|\, W_{j,i} = \left| 2^j \right|_{m_i}^{-}; j = \overline{0, b_1 - 1}; b_1 < b \right\}. \\ i = \overline{1,k}. \qquad (13)$$

В случае, когда базис **M** содержит только один модуль (**M** = {*m*}), индекс *i* в (12), (13) опускается.

Тело алгоритма позиционно-модулярного кодового преобразования по редукционной схеме понижения разрядности вычетов по модулю:

ПМ_РС.1. Положить $b_0 = b$, $X^{(0)} = (x_{b_0-1}^{(0)}\ x_{b_0-2}^{(0)} \dots x_0^{(0)})_2 = (x_{b-1}\, x_{b-2} \dots x_0)_2 = X$, $i = 1$.

ПМ_РС.2. Номеру итерации редукционного процесса присвоить начальные значения: $s = 1$.

ПМ_РС.3. Вычислить $X^{(1)} = \sum_{j=0}^{b_0-1} W_{j,i}(C_i)\, x_j^{(0)}$, сформировав двоичный код $(x_{b_1-1}^{(1)}\ x_{b_1-2}^{(1)} \dots x_0^{(1)})_2$ длины b_1 бит ЦЧ $X^{(1)}$.

ПМ_РС.4. Если $b\_\mathrm{mod}\_i < b_s$, то s инкрементировать ($s = s + 1$), найти

$$X^{(s)} = \sum_{j=0}^{b_{s-1}-2} W_{j,i} x_j^{(s-1)} - W_{b_{s-1}-1,\,i} x_{b_{s-1}-1}^{(s-1)},$$

получая код $(x_{b_{s-1}}^{(s)}\ x_{b_{s-2}}^{(s)}\ x_0^{(s)})_2$ длины b_s бит числа $X^{(s)}$ и данный шаг алгоритма (шаг ПМ_РС.4) повторить сначала.

ПМ_РС.5. Ввиду $b_s \leqslant b\_\mathrm{mod}\_i$ в соответствии с (11) для фиксации искомого значения *i*-й цифры формируемого МК выполнить действия:

ПМ_РС.5А. При $X^{(s)} < 0$ положить $\chi_i = X^{(s)} + m_i$ и перейти к ПМ_РС.6.

ПМ_РС.5Б. В случае $X^{(s)} \geqslant m_i$ положить $\chi_i = X^{(s)} - m_i$ и перейти к ПМ_РС.6.

ПМ_РС.5В. Выполнить операцию присвоения: $\chi_i = X^{(s)}$.

ПМ_РС.6. Если $i \neq k$, то переменную *i* инкрементировать ($i = i + 1$) и перейти к ПМ_РС.2.

ПМ_РС.7. Завершить работу алгоритма.

Приведем демонстрационные примеры.

Пример 1. Пусть требуется найти остаток от деления ЦЧ $X = 987\ 654\ 321$ на модуль $m = 13$.

В целях упрощения расчетов воспользуемся версией алгоритма ПМ_РС.1— ПМ_РС.7, ориентированной на десятичную систему счисления. Сформируем набор необходимых весов:

$$\mathbf{W} = \left\{ W_j \middle| W_j = \left|10^j\right|_m^- ; j = \overline{0, b-1} \right\} =$$
$$= \{ \left|10^0\right|_{13}^-, \left|10^1\right|_{13}^-, \dots, \left|10^8\right|_{13}^- =$$
$$= \{1, -3, -4, -1, 3, 4, 1, -3, -4\}.$$

Выполняя первую итерацию рекурсивной редукционной схемы (4), вычислим

$$X^{(1)} = \sum_{j=0}^{b_0-1} W_j x_j^{(0)} = \sum_{j=0}^{b-1} W_j x_j.$$

Ввиду того, что

$$b_0 = b = 9, X^{(0)} = (x_8^{(0)}\, x_7^{(0)} \dots x_0^{(0)})_{10} =$$
$$= (x_8\, x_7 \dots x_0)_{10} = 987\ 654\ 321$$

имеем:

$$X^{(1)} = 1\cdot 1 + (-3\cdot 2) + (-4\cdot 3) +$$
$$+ (-1\cdot 4) + 3\cdot 5 + 4\cdot 6 + 1\cdot 7 + (-3\cdot 8) + (-4\cdot 9) =$$
$$= 1 - 6 - 12 - 4 + 15 + 24 + 7 - 24 - 36 = -35.$$

Разрядность дополнительного двоичного кода числа $X^{(1)} = -35$ составляет $[\log_2 35] + 1 = 7$ бит, в то время как модуль $m = 13$ является четырехразрядным ($b\_\mathrm{mod} = 4$ бита). Поэтому редукционный процесс (4) должен быть продолжен. Вторая его итерация дает:

$$X^{(2)} = -(5 + (-3\cdot 3)) = 4.$$

Так как $0 < X^{(2)} < m = 13$, то $X^{(2)}$ — искомый остаток. Число итераций редукционного процесса составляет $S = 2$.

Пример 2. Пусть в МСС с базисом $\{m_1, m_2, m_3\} = \{5, 11, 13\}$ требуется найти нормированный остаток $\chi_{3,3} = \left|\mu_{3,3}\chi_3\right|_{m_3}$ для вычета $\chi_3 = 11$ по модулю $m_3 = 13$, где $\mu_{3,3} = \left|M_{3,3}^{-1}\right|_{m_3} = \left|(m_1 m_2)^{-1}\right|_{m_3} = \left|1/(5\cdot 11)\right|_{13} = \left|1/3\right|_{13} = 9$.

В двоичной системе счисления вычет $\chi_3 = 11$ представим в виде $\chi_3 = (x_3\, x_2\, x_1\, x_0)_2 = (1011)_2 = 2^0\cdot 1 + 2^1\cdot 1 + 2^2\cdot 0 + 2^3\cdot 1$. Следуя принятым обозначениям, положим $m = m_3 = 13$, $X = X^{(0)} = \chi_3 = 11$, $b_0 = b = 4$ бита, $C = \mu_{3,3} = 9$, в соответствии с (3) сформируем используемый на первой (начальной) итерации алгоритма ПМ_РС.1— ПМ_РС.7 набор коэффициентов для вычисления сформированного остатка $\chi_{3,3} = |CX|_m = |9\cdot 11|_{13}$:

$$\mathbf{W}(C) = \{W_0(9), W_1(9), W_2(9), W_3(9)\} =$$
$$= \left\{ \left|9\cdot 2^0\right|_{13}^-, \left|9\cdot 2^1\right|_{13}^-, \left|9\cdot 2^2\right|_{13}^-, \left|9\cdot 2^3\right|_{13}^- \right\} =$$
$$= \{ \left|9\cdot 1\right|_{13}^-, \left|9\cdot 2\right|_{13}^-, \left|9\cdot 4\right|_{13}^-, \left|9\cdot 8\right|_{13}^- \} = \{-4, 5, -3, -6\}$$

На первой итерации реализуемого редукционного процесса получаем

$$X^{(1)} = \sum_{j=0}^{b_0-1} W_j(C)\, x_j^{(0)} = \sum_{j=0}^{b-1} W_j(C)\, x_j =$$
$$= (-4\cdot 1) + 5\cdot 1 + (-3\cdot 0) + (-6\cdot 1) = -5.$$

Разрядность абсолютной величины $|X^{(1)}|$ ЦЧ $X^{(1)} = -5$ составляет $b_1 = 3$ бита, а модуль $m = 13$ является четырехбитовым ($b\_mod = 4$ бита). Следовательно, $X^{(1)} \in \mathbf{Z}_{13}^- = \{-6, -5, \dots, 6\}$. Таким образом, выполняемый редукционный процесс состоит из одной итерации ($S = 1$). При этом в соответствии с (11) искомый нормированный

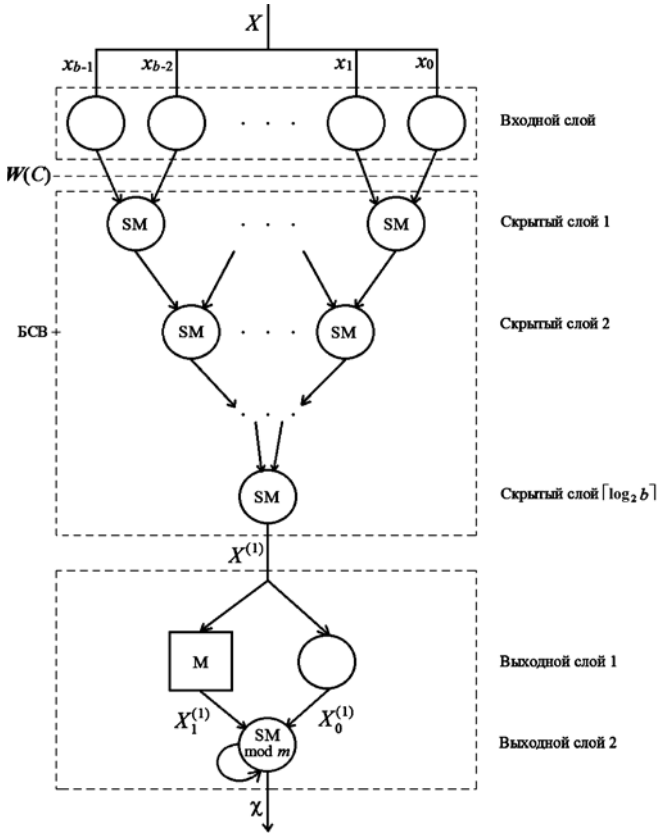
остаток $\chi_{3,3} = X^{(1)} + m = -5 + 13 = 8$, что совпадает с результатом непосредственных вычислений: $\chi_{3,3} = |CX|_m = |9 \cdot 11|_{13} = 8$.

3. Высокоскоростная нейросетевая реализация редукционного алгоритма позиционно-модулярного преобразования больших чисел

Синтезированная процедура ПМ_РС.1—ПМ_РС.7 приведения взвешенных целых чисел к остаткам по модулям $m \in \mathbf{M} = \{m_1, m_2, ..., m_k\}$ ($k \geqslant 1$) может быть реализована как программно, так и аппаратным способом с применением нейросетевой вычислительной технологии [1, 3, 18, 19].

На рисунке представлена структура быстродействующей параллельной НСКК, которая выполняет редукционную схему (4) преобразования $X \to |CX|_m$ за одну итерацию ($S = 1$). Данная нейронная сеть включает входной слой, нейроны которого образуют b-разрядный регистр для фиксации двоичного кода $(x_{b-1}\, x_{b-2} \ldots x_0)_2$ ЦЧ X, $\lceil \log_2 b \rceil$ скрытых слоев, в совокупности составляющих блок суммирования вычетов (БСВ) — взвешенных компонент набора вида (12):

$$\mathbf{W}(C) = \left\{ W_j(C) \,|\, W_j(C) = \left| C 2^j \right|_m^{-}; j = \overline{0, b-1} \right\}, \quad (14)$$



Параллельная нейронная сеть конечного кольца для позиционно-модулярного преобразования по одноитерационной редукционной схеме

а также два выходных слоя, осуществляющих приведение числа $X^{(1)}$ (см. (4)), получаемого блоком суммирования вычетов к остатку по модулю m.

В скрытых слоях используются сумматоры *SM*, которые выполняют операции сложения пар вычетов, формируемых в соответствующих предшествующих слоях. Если в l-й слой БСВ ($l = \overline{1, \lceil \log_2 b \rceil}$) поступает нечетное число N_l вычетов, то вычет, не вошедший в пару (условимся считать, что он имеет порядковый номер N_l) хранится в регистре в течение времени сложения пар вычетов в данном слое. Таким образом, БСВ имеет параллельную древовидную (пирамидальную) архитектуру конвейерного типа. Это обеспечивает получение на выходе БСВ двоичного кода ЦЧ

$$X^{(1)} = \sum_{j=0}^{b_1-1} W_j(C)\, x_j = \sum_{j=0}^{b_1-2} 2^j x_j^{(1)} - 2^{b_1-1} x_{b_1-1}^{(1)} = \\ = \sum_{j=0}^{b_1-2} W_j x_j^{(1)} - W_{b_1-1} x_{b_1-1}^{(1)} \quad (15)$$

(см. (4)) за время $\lceil \log_2 b \rceil t_{\text{сл}}$, где $t_{\text{сл}}$ — длительность операции сложения двух вычетов.

Поскольку в наборе (14) могут быть как положительные, так и отрицательные компоненты, то их суммирование должно проводиться в дополнительном двоичном коде. Согласно оценке (9) разрядность b_1 кода $((x_{b_1-1}^{(1)}\, x_{b_1-2}^{(1)} \ldots x_0^{(1)})_2$ ЦЧ $X^{(1)}$ удовлетворяет неравенству

$$b_1 \leqslant \Delta + b\_\text{mod}\ (\Delta = \lceil \log_2 b \rceil; \\ b\_\text{mod} = \lceil \log_2 m \rceil). \quad (16)$$

Пусть в (16) достигается равенство. Тогда из (15) вытекает соотношение

$$\left| X^{(1)} \right|_m = \left| X_0^{(1)} + X_1^{(1)} \right|_m, \quad (17)$$

где

$$X_0^{(1)} = \sum_{j=0}^{b\_mod-2} 2^j x_j^{(1)} = \sum_{j=0}^{b\_mod-2} W_j x_j^{(1)}; \quad (18)$$

$$X_1^{(1)} = \left| \sum_{j=b\_mod-1}^{\Delta+b\_mod-2} 2^j x_j^{(1)} - 2^{\Delta+b\_mod-1} x_{\Delta+b\_mod-1}^{(1)} \right|_m = \\ = \left| \sum_{j=b\_mod-1}^{\Delta+b\_mod-2} W_j x_j^{(1)} - W_{\Delta+b\_mod-1} x_{\Delta+b\_mod-1}^{(1)} \right|_m. \quad (19)$$

Вычеты W_j ($j = \overline{0, \Delta + b\_mod - 1}$) определяются по (3), (13). Равенства (17)—(19) положены в основу блока приведения ЦЧ $X^{(1)}$ к результирующему остатку $\chi = |X^{(1)}|_m$ по модулю m. Значения b_mod — битового вычета $X_1^{(1)}$ по модулю m рассчитываются предварительно и записываются в

табличную память M по соответствующим адресам:

$$\left(x^{(1)}_{\Delta+b\_mod-1}\, x^{(1)}_{\Delta+b\_mod-2} \dots x^{(1)}_{b\_mod-1}\right)_2,$$

имеющим разрядность $\Delta + 1$ бит. Таким образом, емкость необходимой табличной памяти составляет $2^{\Delta+1} \times b\_mod$ бит.

Согласно вышеизложенному НСКК, представленная на рисунке, работает следующим образом. Двоичный код $(x_{b-1}\, x_{b-2} \dots x_0)_2$ ЦЧ X, подлежащего преобразованию $X \to |CX|_m$, фиксируется в нейронах входного слоя, откуда вместе с набором $\mathbf{W}(C)$ синаптических весов поступает в БСВ. Реализуя рекурсивную $\lceil \log_2 b \rceil$-каскадную процедуру суммирования аддитивных компонент соотношения (15) с весами набора (14) в режиме максимального распараллеливания вычислительного процесса на уровне двухместных операций сложения в скрытых слоях с первого по $\lceil \log_2 b \rceil$-й, БСВ получает дополнительный двоичный код $\left(x^{(1)}_{\Delta+b\_mod-1}\, x^{(1)}_{\Delta+b\_mod-2} \dots x^{(1)}_0\right)_2$ числа $X^{(1)}$. Младшая $b\_\mathrm{mod} - 1$-битовая часть $X^{(1)}_0 = \left(x^{(1)}_{b_{mod}-2}\, x^{(1)}_{b_{mod}-3} \dots x^{(1)}_0\right)_2$ сформированного кода сохраняется в регистре первого выходного слоя, а старшая часть $\left(x^{(1)}_{\Delta+b\_mod-1}\, x^{(1)}_{\Delta+b\_mod-2} \dots x^{(1)}_{b\_mod-1}\right)_2$ подается на адресный вход таблицы M и из нее извлекается остаток $X^{(1)}_1$ от деления старшей части ЦЧ $X^{(1)}$ на m. Вычеты $X^{(1)}_0$ и $X^{(1)}_1$ поступают во второй выходной слой, где параллельный сумматор CM mod m по модулю m с обратной связью выполняет заключительную операцию сложения по модулю m: $\chi = |CX|_m = \left|X^{(1)}\right|_m = \left|X^{(1)}_0 + X^{(1)}_1\right|_m$. В общей сложности редукционная процедура преобразования $X \to |CX|_m$ параллельной НСКК со структурой, приведенной на рисунке, осуществляется за время порядка $(\lceil \log_2 b \rceil + 2)t_{сл}$.

В процессе разработки нейрокомпьютерного обеспечения современных МА-приложений, в том числе криптографических, НСКК играют ключевую роль.

Заключение

Основные результаты представленных в работе прикладных исследований по проблематике создания НСКК для высокопроизводительных МА-приложений в области защиты информации состоят в нижеследующем

1. Для построения нейронных сетей на конечных кольцах вычетов по модулям МСС, как основы нейросетевых модулярных вычислительных структур криптографического назначения, принята редукционная технология позиционно-модулярного преобразования больших чисел с расширенными функциональными возможностями. Обеспечивая оптимальные условия для согласования и реализации фундаментальных свойств параллелизма НС и МА, в рамках развиваемых подходов к решению поставленной задачи применяется также табличный метод ускорения выполняемого рекурсивного процесса поитерационного понижения разрядности формируемых двоичных кодов.

2. Дана математическая формализация редукционного метода позиционно-модулярного кодового преобразования. Получены оценки диапазона изменения, а также разрядности элементов последовательности поитерационных вычетов и на этой основе проведено исследование характера и скорости сходимости применяемой редукционной схемы, предложены эффективные способы сокращения числа итераций выполняемого преобразования.

3. Синтезирован общий алгоритм преобразования взвешенных больших чисел из двоичного в модулярный код по редукционной схеме понижения разрядности элементов формируемой последовательности вычетов. В качестве признака завершения реализуемого рекурсивного процесса по модулям МСС используется фиксация вычетов, разрядности которых достигают значения, отличающегося от разрядностей соответствующих модулей на величину, не превышающую установленный порог.

4. Разработана параллельная структура НСКК, осуществляющей позиционно-модулярное кодовое преобразование по редукционной схеме за одну итерацию — за время порядка $(\lceil \log_2 b \rceil + 2)t_{сл}$ (b — разрядность входного числа; $t_{сл}$ — длительность операции сложения двух вычетов).

Список литературы

1. **Червяков Н. И., Коляда А. А., Ляхов П. А.** и др. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях. М.: Физматлит, 2017. 400 с.

2. **Ananda Mohan P. V.** Residue number systems: Theory and applications. Basel: Birghauser, Mathematics, 2016. 351 p.

3. **Червяков Н. И.** Применение искусственных нейронных сетей и системы остаточных классов в криптографии. М.: Физматлит, 2012. 280 с.

4. **Инютин С. А.** Основы модулярной алгоритмики. Ханты-Мансийск: Полиграфист, 2009. 347 с.

5. **Amos O., Premkumar B.** Residue number systems: Theory and implementation. Singapore: Imperial college press, 2007. 311 p.

6. **Оцоков Ш. А.** Способ организации высокоточных вычислений в модулярной арифметике // Первая международная конференция "Параллельная компьютерная алгебра и ее приложения в новых инфокоммуникационных

системах". Ставрополь, РФ, 20—24 окт., 2014: сборник науч. трудов. Ставрополь: Фабула, 2014. С. 270—277.

7. **Комарова Ю. А., Талалаев И. А.** Аналитический обзор методов и структур для работы с большими данными // Первая международная конференция "Параллельная компьютерная алгебра и ее приложения в новых инфокоммуникационных системах". Ставрополь, РФ, 20—24 окт., 2014: сборник науч. трудов. Ставрополь: Фабула, 2014. С. 477—485.

8. **Афонин М. С.** Способ обработки больших чисел на ПЛИС с малой ресурсной мощностью // Первая международная конференция "Параллельная компьютерная алгебра и ее приложения в новых инфокоммуникационных системах". Ставрополь, РФ, 20—24 окт., 2014: Сборник науч. трудов. Ставрополь: ИИЦ "Фабула", 2014. С. 511—520.

9. **Gulang G.-B., Mao K.-Z., Siew C. K., Huang D.-S.** Fast modular network implementation support vector machines // IEEE Trans. Neural Networks. 2005. Vol. 16, N. 6. P.1651—1663.

10. **Тихонов Э. Е., Евдокимов А. А.** Программно-аппаратная реализация нейронных сетей. Невинномысск: НИЭУП, 2013. 116 с.

11. **Daniela S., Melin P., Castillo O.** Optimization of modular granular neural networks using arhierarchical genetic algorithm based on the database comlexcity applied to human recognition // Informations Sciences. Tjuana Institute of Technology. 2015. Vol. 309. Tjuana, Mexico. P. 73—101.

12. **Кондрашев А. В., Горденко Д. В., Павлюк Д. Н.** Нейронная сеть для преобразования чисел, представленных в позиционном коде, в систему остаточных классов // Исследования в области естественных наук. 2015. № 1. URL: http://science.snauka.ru/2015/01/8925

13. **Бабенко М. Г., Черных А. Н., Кучуков В. А., Дерябин М. А., Кучукова Н. Н.** Разработка нового нейросетевого метода вычисления модульного умножения в системе остаточных классов // Нейрокомпьютеры: разработка и применение. 2016. № 10. С. 41—48.

14. **Коляда А. А.** Обобщенная интегрально-характеристическая база модулярных систем счисления // Информационные технологии. 2017. Т. 23, № 9. С. 641—649.

15. **Чернявский А. Ф., Коляда А. А.** Преобразование кода модулярной системы счисления в обобщенный позиционный код // Доклады НАН Беларуси. 2017. Т. 61, № 4. С. 26—30.

16. **Виноградов И. М.** Основы теории чисел. СПб.: Лань, 2009. 176 с.

17. **Корн Г.** Справочник по математике для научных работников и инженеров. М.: Наука, 1973. 831 с.

18. **Червяков Н. И., Евдокимов А. А.** Нейронные сети конечного кольца для реализации пороговых схем разделения секрета // Нейрокомпьютеры: Разраб., применение. 2007. № 2—3. С. 45—50.

19. **Червяков Н. И., Спельников А. Б., Мезенцева А. Ф.** Нейронная сеть конечного кольца прямого распространения для операций на эллиптических кривых // Нейрокомпьютеры: Разраб., применение. 2008. № 1—2. С. 28—34.

A. A. Kolyada, D. Sc., Associate Professor; E-mail: razan@tut.by,
P. V. Kuchynski, D. Sc., Associate Professor Director of IAPP "Institute of Applied Physics Problems of A. N. Sevchenko" Belarusian State University (IAPP of A. N. Sevchenko), Minsk, 220045, Belarus, Kurchatov St., 7; E-mail: niipfp@bsu.by,
N. I. Chervyakov, D. Sc., Professor, Head of Department, Federal State Autonomous Educational Institution of Higher Professional Education "North-Caucasus Federal University", Stavropol, 355029, Russian Federation; E-mail: Chervyakov@yandex.ru, whbear@yandex.ru

Reducing Method of Positional-Modular Converting Large Numbers for Neural Networks to the End Rings

The article is devoted to the problem of constructing neural networks of a finite ring (NNFR), which serve as the basis for neural network modular computing structures for high-performance cryptographic applications. The methodological basis of the NNFR of the investigated class is the modified reduction method of position-modular transformation of weighted large numbers. The authors give a mathematical formalization of the method, was obtained estimates for the range of change and the number of elements of the residue sequence formed by the reduction scheme of the recursive type, the nature and speed of its convergence are investigated, a flexible tabular mechanism for reducing the number of iterations of the scheme is proposed. Synthesized general reducing algorithm of position-modular code conversion, was developed the parallel structure of the NNFR which performs a basic transformation in one iteration — during the time of order $(\lceil \log_2 b \rceil + 2)t_{сл}$, *where b is the number of the input number;* $t_{сл}$ *is the duration of the two-fold addition operation.*

Keywords: *neural network, neural network of finite ring, synaptic weights, modular number system, modular arithmetic, cryptography, range of large numbers, reduction method of position-modular transformation*

References

1. **Chervjakov N. I., Koljada A. A., Ljahov P. A.** et al. *Moduljarnaja arifmetika i ee prilozhenija v infokommunikacionnyh tehnologijah* [Modular arithmetic and its applications in infocommunication technologies], Moscow, Fizmatlit Publ., 2017, 400 p. (in Russian).

2. **Ananda Mohan P. V.** *Residue number systems: Theory and applications,* Basel, Birghauser, Mathematics, 2016, 351 p.

3. **Chervjakov N. I.** *Primenenie iskusstvennyh nejronnyh setej i sistemy ostatochnyh klassov v kriptografii* [The use of artificial neural networks and the residual class system in cryptography], Moscow, Fizmatlit Publ., 2012, 280 p. (in Russian).

4. **Injutin S. A.** *Osnovy moduljarnoj algoritmiki* [Fundamentals of modular algorithms], Khanty-Mansiysk, Poligrafist Publ., 2009, 347 p. (in Russian).

5. **Amos O., Premkumar B.** *Residue number systems: Theory and implementation*. Singapore, Imperial college press, 2007, 311 p.

6. **Ocokov Sh. A.** The way to organize high-precision calculations in modular arithmetic, *Pervaja mezhdunarodnaja konferencija "Parallel'naja komp'juternaja algebra i ee prilozhenija v novyh infokommunikacionnyh sistemah"* [First International Conference "Parallel Computer Algebra and Its Applications in New Infocommunication Systems"], Stavropol, Russian Federation, 20—24 okt., 2014, Fabula Publ., 2014, pp. 270—277. (in Russian).

7. **Komarova Ju. A., Talalaev I. A.** Analytical review of methods and structures for working with large data, *Pervaja mezhdunarodnaja konferencija "Parallel'naja komp'juternaja algebra i ee prilozhenija v novyh infokommunikacionnyh sistemah"* [First International Conference "Parallel Computer Algebra and Its Applications in New Infocommunication Systems"], *Stavropol, Russian Federation, 20—24 okt., 2014,* Fabula Publ., 2014, pp. 477—485 (in Russian).

8. **Afonin M. S.** The way of processing large numbers on a FPGA with a small resource capacity, *Pervaja mezhdunarodnaja konferencija "Parallel'naja komp'juternaja algebra i ee prilozhenija v novyh infokommunikacionnyh sistemah"* [First International Conference "Parallel Computer Algebra and Its Applications in New Infocommunication Systems"], *Stavropol, Russian Federation, 20—24 okt., 2014,* Fabula Publ., 2014, pp. 511—520 (in Russian).

9. **Gulang G.-B., Mao K.-Z., Siew C. K., Huang D.-S.** Fast modular network implementation support vector machines, *IEEE Trans. Neural Networks*, 2005, vol. 16, no. 6, pp. 1651—1663.

10. **Tihonov Je. E., Evdokimov A. A.** *Programmno-apparatnaja realizacija nejronnyh setej* [Software and hardware implementation of neural networks: Monograph], Nevinnomyssk, NIJeUP Publ., 2013, 116 p. (in Russian).

11. **Daniela S., Melin P., Castillo O.** Optimization of modular granular neural networks using arhierarchical genetic algorithm based on the database comlexcity applied to human recognition, *Informations Sciences. Tjuana Institute of Technology*, 2015, Vol. 309, Tjuana, Mexico, pp. 73—101.

12. **Kondrashjov A. V., Gordenko D. V., Pavljuk D. N.** Neural network for converting the numbers represented in the positional code to the residual class system. *Issledovanija v oblasti estestvennyh nauk* [Research in the field of natural sciences], 2015, no. 1, available at: http://science.snauka.ru/2015/01/8925 (in Russian).

13. **Babenko M. G., Chernyh A. N., Kuchukov V. A., Derjabin M. A., Kuchukova N. N.** Development of a new neural network method for calculating modular multiplication in a system of residual classes, *Nejrokomp'jutery: razrabotka i primenenie* [Neurocomputers: development and application], 2016, no. 10, pp. 41—48 (in Russian).

14. **Koljada A. A.** Generalized integral-characteristic base of modular number systems, *Informacionnye tehnologii* [Information Technology] 2017, vol. 23, no. 9, pp. 641—649 (in Russian).

15. **Chernjavskij A. F., Koljada A. A.** Conversion of a modular number system code to a generalized positional code, *Doklady NAN Belarusi* [Reports of NASc of Belarus], 2017, vol. 61, no. 4, pp. 26—30 (in Russian).

16. **Vinogradov I. M.** *Osnovy teorii chisel* [Fundamentals of number theory], St. Petersburg, Lan' Publ., 2009, 176 p. (in Russian).

17. **Korn G.** *Spravochnik po matematike dlja nauchnyh rabotnikov i inzhenerov* [A handbook on mathematics for scientists and engineers], Moscow, Nauka Publ., 1973, 831 p. (in Russian).

18. **Chervjakov N. I., Evdokimov A. A.** Neural networks of the finite ring for the implementation of threshold separation schemes for secretion, *Nejrokomp'jutery: Razrab., primenenie* [Neurocomputers: Development, application], 2007, no. 2—3, pp. 45—50 (in Russian).

19. **Chervjakov N. I., Spel'nikov A. B., Mezenceva A. F.** Neural network of a finite ring of direct propagation for operations on elliptic curves, *Nejrokomp'jutery: Razrab., primenenie* [Neurocomputers: Development, application], 2008, no. 1—2, pp. 28—34 (in Russian).

Адрес редакции:

107076, Москва, Стромынский пер., 4

Телефон редакции журнала **(499) 269-5510**
E-mail: it@novtex.ru

Технический редактор *Е. В. Конова.*
Корректор *Е. В. Комиссарова.*
Сдано в набор 07.03.2018. Подписано в печать 26.04.2018. Формат 60×88 1/8. Бумага офсетная.
Усл. печ. л. 8,86. Заказ IT518. Цена договорная.

Журнал зарегистрирован в Министерстве Российской Федерации по делам печати, телерадиовещания и средств массовых коммуникаций.
Свидетельство о регистрации ПИ № 77-15565 от 02 июня 2003 г.

Оригинал-макет ООО "Адвансед солюшнз". Отпечатано в ООО "Адвансед солюшнз".
119071, г. Москва, Ленинский пр-т, д. 19, стр. 1.