ISSN 1816-0301 (print)
УДК 004.9, 004.94, 004.56

Поступила в редакцию 22.01.2018
Received 22.01.2018

Н. И. Червяков[1], А. А. Коляда[2], Н. А. Коляда[2], В. А. Кучуков[1], С. Ю. Протасеня[2]

[1]Северо-Кавказский федеральный университет, Ставрополь, Россия
[2]Научно-исследовательское учреждение «Институт прикладных физических проблем имени А. Н. Севченко» Белорусского государственного университета, Минск, Беларусь

НЕЙРОННЫЕ СЕТИ КОНЕЧНОГО КОЛЬЦА НА ОСНОВЕ РЕДУКЦИОННОЙ СХЕМЫ ПОЗИЦИОННО-МОДУЛЯРНОГО КОДОВОГО ПРЕОБРАЗОВАНИЯ

Аннотация. Рассматривается проблема создания нейросетевых модулярных вычислительных структур для высокопроизводительных выражений в области защиты информации. Главное внимание уделяется редукционной технологии позиционно-модулярного преобразования масштабируемых целых чисел, которая служит основой для построения так называемых нейронных сетей конечного кольца (НСКК). Для повышения скорости сходимости используемой редукционной схемы понижения разрядности элементов формируемой последовательности вычетов предложен эффективный табличный метод. Разработанный подход позволяет свести к теоретическому минимуму количество итераций редукционного процесса. Это достигается за счет применения гибкого адаптивного механизма проверки принадлежности поитерационных вычетов к специальному диапазону, допускающему табличную декомпозицию его элементов на пары остатков по модулям модулярной системы счисления. На базе модифицированного редукционного метода синтезированы быстрый алгоритм и параллельная структура НСКК с обратной связью, обеспечивающая реализацию редукционной схемы за время $(S(\lceil \log_2 b \rceil + 1) + 2)t_{\text{сл}}$, где S – число итераций, b – разрядность входного числа, $t_{\text{сл}}$ – длительность операции сложения двух вычетов.

Ключевые слова: нейронная сеть, нейронная сеть конечного кольца, нейронная сеть с обратной связью, синаптические веса, модулярная система счисления, модулярная арифметика, редукционная схема понижения разрядности чисел, табличный метод

Для цитирования. Нейронные сети конечного кольца на основе редукционной схемы позиционно-модулярного кодового преобразования / Н. И. Червяков [и др.] // Информатика. – 2018. − Т. 15, № 2. – С. 98–110.

N. I. Chervyakov[1], A. A. Kolyada[2], N. A. Kolyada[2], V. A. Kuchukov[1], S. U. Protasenia[2]

[1]North-Caucasus Federal University, Stavropol, Russia
[2]Scientific Research Institution "Institute of Applied Physical Problems named after A. N. Sevchenko" of the Belarusian State University, Minsk, Belarus

NEURAL NETWORKS OF THE FINAL RING BASED ON THE REDUCTION SCHEME OF THE POSITION-MODULAR-CODE TRANSFORMATION

Abstract. The article studies the problem of creating a neural network of modular computing structures for high-performance expressions in the field of information security. The main attention is paid to the reduction technology of position-modular transformation of scalable integers, which serves as the basis for constructing the so-called neural networks of the finite ring (NNFR). To increase the speed of convergence of the reduction scheme used to reduce the number of elements of the generated sequence of residues, an effective tabular method is proposed. The developed approach makes it possible to reduce the number of iterations of the reduction process to a theoretical minimum. This is achieved through flexible adaptive mechanism check botheration deductions to a special range, allowing a tabular decomposition of its elements into pairs of residues in modules of the modular number system. On the basis of a modified reduction method there was synthesized a fast algorithm and a parallel structure of the NNFR with feedback, which ensures the implementation of the reduction scheme in a time order $(S(\lceil \log_2 b \rceil + 1) + 2)t_{sum}$, were S – the number of iterations, b – the bit width of the input number, t_{sum} – the duration of the addition operation of two deductions.

Keywords: neural network, neural network end rings, a neural network with feedback, the synaptic weight, modular number system, modular arithmetic, reducing the scheme of reduction of bit numbers, the table method

For citation. Chervyakov N. I., Kolyada A. A., Kolyada N. A., Kuchukov V. A., Protasenia S. U. Neural networks of the final ring based on the reduction scheme of the position-modular-code transformation. *Informatics*, 2018, vol. 15, no. 2, pp. 98–110 (in Russian).

Введение. Как известно, важнейшей неотъемлемой составляющей математического и компьютерного обеспечения современных систем защиты информации являются вычислительные технологии на диапазонах больших чисел (ДБЧ). Особое место среди таких технологий занимают модулярные вычислительные технологии (МВТ) [1–6]. Обладая естественным кодовым параллелизмом, модулярные вычислительные структуры имеют ряд существенных преимуществ над позиционными структурами, и наиболее ярко эти преимущества проявляются при оперировании в ДБЧ. Важным фактором, способствующим неуклонному повышению уровня востребованности технологий требуемого класса на основе модулярной арифметики (МА), является их идеальная приспособленность к нейросетевым реализациям [1, 3, 7–11].

Активно развиваемое в настоящее время новое направление фундаментальных и прикладных исследований в криптографии, нацеленное на как можно более полную реализацию оптимально согласованных свойств параллелизма нейронных сетей (НС) и арифметики модулярных систем счисления (МСС), предоставляет принципиально новые возможности для построения высокопроизводительных криптосистем различного функционального назначения. Многообещающие перспективы совместного применения модулярной и нейросетевой вычислительных технологий обусловлены тем, что при согласованном числе синапсов НС, используемых в процессе взаимодействия ее нейронов, и мощности модулярного базиса сеть становится естественным представлением применяемой МСС. На отмеченное обстоятельство указывают, в частности, следующие признаки:

– семантическое сходство позиционных форм модулярных чисел [1, 10, 12, 13] с расчетными соотношениями формального нейрона [3, 10];

– 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 ассоциативной нейронной памяти.

Основополагающая идея осуществляемых разработок по созданию методологического, алгоритмического и программно-аппаратного обеспечения нейросетевой МВТ состоит в переводе вычислений из ДБЧ в компьютерные диапазоны целых чисел (ЦЧ) стандартной разрядности. Ключевую роль в процессе решения сформулированной задачи выполняют НС на конечных кольцах вычетов по рабочему базису модулей [1, 3, 14, 15]. Операционную основу НСКК составляют главным образом операции приведения ЦЧ к остаткам по используемым модулям. Как структурно, так и на операционном уровне НСКК максимально должны быть согласованы с естественным кодовым параллелизмом МА. В полной мере данному условию удовлетворяет рассматриваемый в данной статье редукционный метод позиционно-модулярного кодового преобразования.

Редукционный метод позиционно-модулярного преобразования масштабируемых целых чисел. Введем обозначения:

$\mathbf{Z}$ – множество ЦЧ;

$\lfloor a \rfloor$ и $\lceil a \rceil$ – наибольшее и наименьшее ЦЧ соответственно, не большие и не меньшие вещественной величины a;

$\mathbf{Z}_m = \{0, 1, \ldots, m-1\}$, $\mathbf{Z}_m^{-} = \{-\lfloor m/2 \rfloor, -\lfloor m/2 \rfloor+1, \ldots, \lceil m/2 \rceil -1\}$ – 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;

$\mathbf{M}=\{m_1, m_2, \ldots, m_k\}$ – набор модулей базовой МСС (модулярный базис), где k – мощность базиса;

$\mathbf{X}=\left(|X|_{m_1}, |X|_{m_2}, \ldots, |X|_{m_k}\right)$ – представление ЦЧ X в МСС с базисом $\mathbf{M}$.

Традиционно в качестве операционной основы НСКК используется преобразование ЦЧ X из двоичной системы счисления в модулярную [3, 14, 15]. Принимая, однако, во внимание то обстоятельство, что при построении различных конфигураций МА важную роль выполняют преобразования масштабируемых вычетов в остатке по модулям МСС, в настоящей статье рас-

сматривается расширенный класс НСКК, которые осуществляют требуемые операции – преобразования вида $X\to |CX|_m$, где X – неотрицательное ЦЧ, заданное своим двоичным кодом $(x_{b-1}\ x_{b-2}\ \dots\ x_0)_2$ разрядностью b бит ($x_j\in\{0,1\}$ $(j=\overline{0,b-1})$); C – целочисленная константа (масштабирующий множитель); $m\in\mathbf{M}$. По критерию простоты нейросетевой реализации наиболее приемлемым методом выполнения преобразования $X\to |CX|_m$ является метод модулярной редукции по рекурсивной схеме последовательного снижения разрядности элементов формируемой последовательности вычетов [1, 3, 15].

Положим

$$X^{(0)}=(x_{b_0-1}^{(0)}\ \ x_{b_0-2}^{(0)}\dots x_0^{(0)})_2=\sum_{j=0}^{b_0-1}2^j x_j^0\ \ (b_0=b,\ \ x_j^{(0)}=x_j) \tag{1}$$

и пусть

$$W_j(C)=\left|C\cdot 2^j\right|_{m_0}^{-}=\begin{cases}\left|C\cdot 2^j\right|_m, \text{если } \left|C\cdot 2^j\right|_m<\left\lceil\frac{m}{2}\right\rceil,\\ \left|C\cdot 2^j\right|_m-m, \text{если } \left|C\cdot 2^j\right|_m\geq\left\lceil\frac{m}{2}\right\rceil,\end{cases} \tag{2}$$

$$\left(j=\overline{0,b-1}\right).$$

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

Применяемая редукционная схема описывается операционной последовательностью

$$\left\langle X^{(1)}=\sum_{j=0}^{b_0-1}W_j(C)x_j^{(0)}=(x_{b_1-1}^{(1)}\ x_{b_1-2}^{(1)}\dots x_0^{(1)})_2-2^{b_1}x_{b_1-1}^{(1)}=\sum_{j=0}^{b_1-2}2^j x_j^{(1)}-2^{b_1-1}x_{b_1-1}^{(1)},\right.$$

$$X^{(s)}=\textstyle\sum_{j=0}^{b_{s-1}-2}W_j x_j^{(s-1)}-W_{b_{s-1}-1}x_{b_{s-1}-1}^{(s-1)}=(x_{b_s-1}^{(s)}\ \ x_{b_s-2}^{(s)}\ \ \dots\ \ x_0^{(s)})_2-2^{b_s}x_{b_s-1}^{(s)}= \tag{3}$$

$$\left.=\sum_{j=0}^{b_s-2}2^j x_j^{(s)}-2^{b_s-1}x_{b_s-1}^{(s)}\quad (s=\overline{2,S});\right\rangle,$$

$$\chi=\left|X^{(S)}\right|_m$$

где b_1 и b_s – длины дополнительных двоичных кодов $(x_{b_1-1}^{(1)}\ x_{b_1-2}^{(1)}\dots x_0^{(1)})_2$ и $(x_{b_s-1}^{(s)}\ x_{b_s-2}^{(s)}\ \dots\ x_0^{(s)})_2$ соответственно ЦЧ $X^{(1)}$ и $X^{(s)}$, которые, как следует из (2), в принципе могут быть и отрицательными; S – количество итераций схемы.

Основополагающая идея редукционного метода, реализуемая в рамках вычислительной схемы (3) в целях приведения ЦЧ CX к остатку по модулю m, состоит в замене коэффициентов $C2^j$ правой части равенства CX=$CX^{(0)}=\sum_{j=0}^{b_0-1}(C2^j)x_j^{(0)}$ на вычеты $W_j(C)$, определяемые по правилу (2), а коэффициентов 2^j, $2^{b_{s-1}-1}$ выражения $X^{(s)}=\sum_{j=0}^{b_{s-1}-2}2^j x_j^{(s-1)}-2^{b_{s-1}-1}x_{b_{s-1}-1}^{(s-1)}$ – на вычеты W_j , $W_{b_{s-1}-1}$ при $s=\overline{2,S}$. Ввиду (2) все получаемые после указанных замен ЦЧ $X^{(s)}$ $(s=\overline{1,S})$ равноостаточны по модулю m. Они являются элементами одного и того же класса $\overline{X}$ вычетов по данному модулю: $\mathbf{R}_m(CX)=\{R\in\boldsymbol{Z}|R\equiv CX(\mathbf{mod}\ m)\}$.

Справедливо следующее утверждение.

Теорема. *Пусть модуль m является простым числом (m>2) и имеет разрядность b_mod =* $=\lceil log_2 m\rceil$ *бит. Тогда для длины* b_s *дополнительного двоичного кода* $(x_{b_s-1}^{(s)}\ x_{b_s-2}^{(s)}\ \dots\ x_0^{(s)})_2$ *вы-*

чета $X^{(s)}$, определяемого по редукционной схеме (3) для входного ЦЧ (1) с использованием синаптических весов (2), верна оценка

$$b_s < b\_mod + \log_2 b_{s-1}, \tag{4}$$

где b_{s-1} – разрядность ЦЧ $X^{(s-1)}, s = \overline{1,S}$.

При этом количество S итераций редукционной схемы (3) удовлетворяет неравенству

$$S \le \min\{s \mid b_s - b\_mod < \\ < \log_2\left(b\_mod + \log_2\left(b\_mod + \log_2(\dots log_2(b\_mod + \log_2 b_0)\dots)\right)\right) \le \\ \le \Delta_{min}; s \ge 1\}\,(b_0 = b), \tag{5}$$

где Δ_{min} – установленный порог.

Доказательство. Как известно, множество всех степеней числа 2 по модулю m в мультипликативной группе кольца $\mathbf{Z}_m$ образует 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 (2) набору вычетов:

$$\{W_j \in \mathbf{Z}_m^- \mid W_j = \left|2^j\right|_m^-; j = \overline{0, N-1}\}. \tag{6}$$

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

$$\{W_0, W_1, \dots, W_{N-1}, W_N, \dots, W_{b_{s-1}-1}\} \quad (s = \overline{2,S}), \tag{7}$$

используемые в (3), имеют циклическую структуру. Сегменты длины N в (7) с начальными элементами W_{iN} $(i = \overline{0, \lfloor b_{s-1}/N \rfloor - 1})$ совпадают с последовательностью (6). В случае, когда b_{s-1} не делится нацело на N, последний $\lfloor b_{s-1}/N \rfloor$-й сегмент в (7) оказывается неполным. Пусть N_+ и N_- – количество соответственно положительных и отрицательных вычетов в множестве (6). Тогда с учетом вышеизложенного при $s = \overline{2,S}$ максимально возможное значение числа $X^{(s)}$ (см. (3)) сверху можно оценить следующим образом:

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

$$= \frac{b_{s-1}}{N}(m - N_+)\frac{N_+}{2}.$$

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

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

$$= \frac{b_{s-1}}{N}\left(-\frac{m-1}{2} - \frac{m-1}{2} + N_- - 1\right)\frac{N_-}{2} =$$

$$= -\frac{b_{s-1}}{N}(m - N_-)\frac{N_-}{2}.$$

Следовательно,

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

$$= \frac{b_{s-1}}{N}\left(\frac{m}{2}(N_+ + N_-) - \frac{N_+^2 + N_-^2}{2}\right) =$$

$$= \frac{b_{s-1}}{2N}\left(mN - (N_+^2 + N_-^2 + 2N_+N_- - 2N_+N_-)\right) =$$

$$= \frac{1}{2}b_{s-1}\left(m - \frac{(N_+ + N_-)^2}{N} + \frac{2N_+N_-}{N}\right) =$$

$$= \frac{1}{2}b_{s-1}\left(m - N + 2N\left(\left(\frac{N_+}{N}\cdot\frac{N_-}{N}\right)^{\frac{1}{2}}\right)^2\right) \le$$

$$\le \frac{1}{2}b_{s-1}\left(m - N + 2N\left(\frac{N_+}{N} + \frac{N_-}{N}\right)\cdot\frac{1}{4}\right) =$$

$$= \frac{1}{2}b_{s-1}\left(m - N + \frac{1}{2}N\right) = \frac{1}{2}b_{s-1}\left(m - \frac{1}{2}N\right).$$

Так как N является делителем функции Эйлера $\varphi(m) = m-1$, оно представимо в виде $N = (m-1)/d$, где d – делитель ЦЧ $\varphi(m) = m-1$ ($d \neq N$). С учетом отмеченного обстоятельства из оценки для $\max\{X^{(s)}\} - \min\{X^{(s)}\}$ получаем

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

Отсюда следует

$$\log_2\left(\max\{X^{(s)}\} - \min\{X^{(s)}\} + 1\right) + 1 <$$

$$< \log_2(b_{s-1}) + b\_\mathrm{mod} + \log_2\left(1 - \tfrac{1}{2d} + \tfrac{1}{2dm}\right).$$

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

$$b_s = \left\lceil \log_2(\max\{X^{(s)}\} - \min\{X^{(s)}\} + 1)\right\rceil < b\_mod\ + \log_2(b_{s-1}).$$

Что касается числа $X^{(1)}$ (см. (3)), то для оценки его разрядности b_1 также применим рассмотренный выше подход. Таким образом, при любом целочисленном C последовательность $\{W_0(C), W_1(C), \dots, W_{N-1}(C), W_N(C), W_{N+1}(C), \dots, W_{2N-1}(C), \dots, W_{b_0-1}(C)\}$ абсолютно наименьших остатков по модулю m, определяемых по правилу (2), благодаря выполнению равенств $W_{iN+j}(C) = W_j(C)\left(i = \overline{1, \left\lfloor \frac{b_0}{N} \right\rfloor - 1};\ j = \overline{0, N-1}\right)$ и последовательности (7) обладает циклической структурой (с периодом N). Математические выкладки, приведенные выше для $X^{(s)}$ $(s = \overline{2, S})$, имеют вид $b_1 < b\_mod\ + \log_2 b_0 = b\_mod\ + \log_2 b$.

Существование искомого числа S итераций редукционной схемы, удовлетворяющего условию (5), вытекает из оценки (4), записанной в развернутом виде (по рекуррентному правилу), и выбора порога Δ_{min}. ■

Замечание 1. Фигурирующий в (5) порог Δ_{min} подбирается экспериментально так, чтобы последовательность b_0, b_1, …, b_S была строго убывающей. Выполнение данного условия обеспечивается тем, что при S, удовлетворяющем (5), величины $\log_2 b_0$, $\log_2 b_1$, …, $\log_2 b_S$ образуют убывающую последовательность.

Замечание 2. В соответствии с (5) и замечанием 1 в качестве признака завершения редукционного процесса (3), естественно, следует принять выполнение неравенства

$$\Delta_S = b_S - b\_mod \le \Delta_{min}. \tag{8}$$

При использовании в (8) Δ_{min}= 0 искомое значение выходной величины схемы (3) формируется по правилу

$$\chi = \begin{cases} X^{(S)} + m, \text{если } X^{(S)} < 0, \\ X^{(S)}, \text{если } 0 \le X^{(S)} < m, \\ X^{(S)} - m, \text{если } m \le X^{(S)}. \end{cases} \tag{9}$$

Замечание 3. Расчетные соотношения схемы (3) целиком согласуются с принципами нейросетевой вычислительной технологии. При суммировании синаптических весов (2) с последующим вычислением активационной функции $\chi = |CX|_m = \left|X^{(S)}\right|_m$, реализуемой, например, в виде (9), набор необходимых весовых коэффициентов (2) рассчитывается предварительно и хранится в памяти.

Табличный метод ускоренной реализации редукционной схемы. С увеличением значения переменной s скорость приближения b_S к разрядности b_mod модуля m снижается (см. (4), (5)). Поэтому в целях уменьшения количества S итераций вычислительной схемы (3) до приемлемого уровня в (8) следует использовать выбираемый надлежащим образом порог $\Delta_{min} > 0$. При этом необходимо учитывать то обстоятельство, что с ростом Δ_{min} расчетное соотношение для активационной функции нейронной сети в сравнении с (9) становится более сложным. Выбор наиболее приемлемых конфигураций блока суммирования синаптических весов, активационной функции $f(F^{(s)})$ базового нейрона ($s = \overline{1,S}$), способа ее реализации и организации цикла по переменной x является ключевым аспектом задачи оптимизации объема производимых вычислений и соответствующих реализационных затрат для формирования последовательности вычетов $X^{(1)}$, $X^{(2)}$, … $X^{(S)}$, а также генерирования и анализа по правилу типа (8) на каждой итерации признака окончания рекурсивного процесса (3). Представляемый подход к построению НСКК предусматривает применение табличного метода ускоренного выполнения рекурсивной редукционной схемы (3). Предлагаемый метод обеспечивает уменьшение числа S итераций схемы и снижение сложности активационной функции до уровня сложности расчетного соотношения (9).

Разобьем b_s – битовый дополнительный двоичный код $(x^{(s)}_{b_{s-1}}\ x^{(s)}_{b_{s-2}}\ \dots\ x^{(s)}_0)_2$ ЦЧ $X^{(s)}$ – на три части: младшую $(x^{(s)}_{b\_mod-2}\ x^{(s)}_{b\_mod-3}\ \dots\ x^{(s)}_0)_2$, среднюю $(x^{(s)}_{b\_mod+\Delta_{min}-1}\ x^{(s)}_{b\_mod+\Delta_{min}-2}\ \dots\ x^{(s)}_{b\_mod-1})_2$ и старшую $(x^{(s)}_{s-1}\ x^{(s)}_{s-2}\ \dots\ x^{(s)}_{b\_mod+\Delta_{min}})_2$, которые имеют соответственно разрядности b_mod-1, $\Delta_{min}+1$ и $\Delta' = \Delta - \Delta_{min}$ ($\Delta = b_s - b\_mod$). Основополагающая идея табличного метода ускоренного выполнения редукционного процесса (3) состоит в увеличении порога Δ_{min} до максимально допустимого (с точки зрения размера используемой таблицы) значения, обеспечивающего минимизацию количества S итераций реализуемой схемы. На искомую заключительную итерацию редукционного процесса указывает нулевое значение управляющего сигнала

$$\Gamma = \left| \left(\bigvee_{j=b_s-\Delta'-1}^{b_s-1} x_j^{(s)} \right) + \left(\bigwedge_{j=b_s-\Delta'-1}^{b_s-1} x_j^{(s)} \right) \right|_2 . \tag{10}$$

Булево выражение (10) фактически представляет собой реализацию проверки условия (8) из выражения (2). Значение Г=0 сигнала (10) указывает на то, что все разряды старшей Δ' битовой части $(x_{b_s-1}^{(s)}\ x_{b_s-2}^{(s)}\ \dots\ x_{b_s-\Delta'-1}^{(s)})_2$ дополнительного двоичного кода $(x_{b_s-1}^{(s)}\ x_{b_s-2}^{(s)}\ \dots\ x_0^{(s)})_2$ вычета $X^{(s)}$ совпадают со старшим разрядом в средней части $(x_{b\_mod+\Delta_{min}-1}^{(s)}\ x_{b\_mod+\Delta_{min}-2}^{(s)}\ \dots\ x_{b\_mod-1}^{(s)})_2$ данного кода:

$$x_j^{(s)} = x_{b_s-\Delta'}^{(s)} = x_{b\_mod+\Delta_{min}-1}^{(s)} \quad (j = \overline{b_s-\Delta'-1,\ b_s-1}). \tag{11}$$

При выполнении условия (11) ЦЧ $X^{(s)}$ является элементом диапазона $\boldsymbol{Z}_{2^{b_{mod}+\Delta_{min}-1}}^{-} = \{-2^{b\_mod+\Delta_{min}-1}, -2^{b\_mod+\Delta_{min}-1}+1, \dots, 2^{b\_mod+\Delta_{min}-1}-1\}$. При этом $X^{(s)}$ полностью определяется дополнительным двоичным кодом $(x_{b\_mod+\Delta_{min}-1}^{(s)}\ ,\ x_{b\_mod+\Delta_{min}-2}^{(s)}\ , \dots, x_0^{(s)})_2$ и, следовательно,

$$X^{(s)} = \sum_{j=0}^{b\_mod+\Delta_{min}-2} 2^j x_j^{(s)} - 2^{b\_mod+\Delta_{min}-1} x_{b\_mod+\Delta_{min}-1}^{(s)}. \tag{12}$$

По достижении итерации, на которой фиксируется Г=0, текущее значение s присваивается переменной S. В этом случае из (12) для $X^{(S)}$ получаем соотношение

$$\left|X^{(S)}\right|_m = \left|X_0^{(S)} + X_1^{(S)}\right|_m, \tag{13}$$

где

$$X_0^{(S)} = \sum_{j=0}^{b\_mod-2} 2^j x_j^{(S)} = \sum_{j=0}^{b\_mod-2} W_j x_j^{(S)}; \tag{14}$$

$$X_1^{(S)} = \left| \sum_{j=b\_mod-1}^{b\_mod+\Delta_{min}-2} 2^j x_j^{(S)} - 2^{b\_mod+\Delta_{min}-1} x_{b\_mod+\Delta_{min}-1}^{(S)} \right|_m = \tag{15}$$

$$= \left| \sum_{j=b\_mod-1}^{b\_mod+\Delta_{min}-2} W_j x_j^{(S)} - W_{b\_mod+\Delta_{min}-1} x_{b\_mod+\Delta_{min}-1}^{(S)} \right|_m.$$

Значения b_mod – битового вычета $X_1^{(S)}$ по модулю m – рассчитываются согласно (15) предварительно и записываются в табличную память (таблицу *TRes_MP*) по правилу

$$TRes\_MP\ [\left(x_{b\_mod+\Delta_{min}-1}^{(S)}\ x_{b\_mod+\Delta_{min}-2}^{(S)}\ \dots\ x_{b\_mod-1}^{(S)}\ \right)_2] = X_1^{(S)}. \tag{16}$$

Емкость таблицы *TRes_MP* составляет $2^{\Delta_{min}+1}$ слов с разрядностью b_mod бит.

В случае, когда управляющий сигнал Г, генерируемый по формуле (10), принимает значение Г=1, реализация редукционной схемы (3) продолжается при очередном значении s.

Приведение ЦЧ $X^{(S)}$ к результирующему остатку по модулю m описанным табличным методом на основе (13)–(16) позволяет значительно расширить диапазон анализируемых вычетов при генерировании признака завершения редукционного процесса. Именно это обстоятельство и обеспечивает существенное уменьшение числа S итераций вычислительной схемы (3).

Редукционный алгоритм ускоренного позиционно-модулярного преобразования масштабируемых целых чисел. На базе представленного метода последовательного уменьшения разрядности ЦЧ по редукционной схеме (3) рекурсивного типа синтезирован алгоритм

ускоренного позиционно-модулярного кодового преобразования, ориентированный на нейросетевую реализацию.

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_mod_i*=$\lceil \log_2 m_i \rceil$ $\left(i = \overline{1,k}\right)$; $k \geq 1$);

– порог $\Delta_{min} > 0$ для решающего правила завершения редукционного процесса.

Входные данные:

– двоичный код $(x_{b-1}\ x_{b-2}\ \ldots\ x_0)_2$ исходного ЦЧ X (b – длина кода);

– целочисленные коэффициенты C_i произведений C_iX, подлежащих приведению к остаткам по модулям m_i $\left(i = \overline{1,k}\right)$.

Выходные данные: модулярный код $(\chi_1, \chi_2, \ldots, \chi_k)$ $(\chi_i = |C_iX|_{m_i}\left(i = \overline{1,k}\right))$ по заданному базису модулей – **M**={m_1, m_2, …, m_k}.

Предварительно получаемые данные:

1. Рассчитанные согласно правилу (2) наборы весов

$$\mathbf{W}_i(C) = \left\{W_{j,i}(C)\middle| W_{j,i}(C) = \left|C_i 2^j\right|_{m_i}^{-}; j = \overline{0, b-1}\right\}; \tag{17}$$

$$\mathbf{W}_i = \left\{W_{j,i}\middle| W_{j,i} = \left|2^j\right|_{m_i}^{-}; j = \overline{0, b_1 - 1}\,; b_1 < b\right\}\left(i = \overline{1,k}\right). \tag{18}$$

2. Таблицы *TRes_MP_*1, *TRes_MP_*2, …., *TRes_MP_k* остатков от ЦЧ вида

$$A_i\left(a_0, a_1, \ldots, a_{\Delta_{min}}\right) = \sum_{j=0}^{\Delta_{min}-1} W_{j+b\_mod\_i-1}a_j - W_{\Delta_{min}+b\_mod\_i-1}a_{\Delta_{min}}$$

по модулям m_i (см. (15), (16)), генерируемые согласно правилу

$$TRes\_MP\_i[(a_{\Delta_{min}}\ a_{\Delta_{min}-1} \ldots a_0)_2] = \left|A_i(a_0,\ a_1, \ldots, a_{\Delta_{min}})\right|_{m_i}\ (a_j \in \{0,1\}\ (j = \overline{0, \Delta_{min}}); i = \overline{1,k}). \tag{19}$$

В случае, когда базис **M** содержит только один модуль (**M**={m}), индекс i в (17), (18) опускается.

Алгоритм позиционно-модулярного кодового преобразования по высокоскоростной редукционной схеме понижения разрядности вычетов по модулю состоит из следующих шагов:

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

_ПМ_РС.2. Номеру итерации редукционного процесса присвоить начальное значение s=1.

_ПМ_РС.3. Следуя (3), с учетом (17) вычислить $X^{(1)} = \sum_{j=0}^{b_0-1} W_{j,i}\,(C_i)x_j^{(0)}$, сформировав двоичный код $(x_{b_1-1}^{(1)}\ x_{b_1-2}^{(1)}\ \ldots\ x_0^{(1)})_2$ длиной b_1 бит ЦЧ $X^{(1)}$.

_ПМ_РС.4. По старшей $(b_s - b\_mod\_i - \Delta_{min} + 1)$-битовой части $(x_{b_s-1}^{(s)}\ \ x_{b_s-2}^{(s)}\ \ldots\ x_{b\_mod\_i+\Delta_{min}-1}^{(s)})_2$ двоичного кода $(x_{b_s-1}^{(s)}\ x_{b_s-2}^{(s)} \ldots\ x_0^{(s)})_2$ ЦЧ $x^{(s)}$ получить булеву величину

$$\Gamma = \left|\left(\bigvee_{j=b\_mod\_i+\Delta_{min}-1}^{b_s-1} x_j^{(s)}\right) + \left(\bigwedge_{j=b\_mod\_i+\Delta_{min}-1}^{b_s-1} x_j^{(s)}\right)\right|_2.$$

_ПМ_РС.5. Если Г=1, то инкрементировать s (s:=s+1), найти

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

получив код $(x_{b_{s-1}}^{(s)} \; x_{b_{s-2}}^{(s)} \;\; x_0^{(s)})_2$ длиной b_s бит числа $X^{(s)}$, и перейти к _ПМ_РС.4.

_ПМ_РС.6. Ввиду Г=0 в соответствии с (13) – (16), (18), (19) переменной S присвоить значение $S=s$ и для фиксации искомого значения i-й цифры формируемого модулярного кода выполнить следующие действия:

_ПМ_РС.6А. Рассчитать вычет

$$X_0^{(S)} = \sum_{j=0}^{b\_mod\_i-2} 2^j x_j^{(S)} = \sum_{j=0}^{b\_mod\_i-2} W_{j,i} x_j^{(S)}.$$

_ПМ_РС.6Б. Из таблицы *TRes_MP_i* извлечь вычет

$$X_1^{(S)} = \text{TRes\_MP}\_i[(x_{b\_mod\_i+\Delta_{min}-1}^{(S)} \; x_{b\_mod\_i+\Delta_{min}-2}^{(S)} \; \dots \; x_{b\_mod\_i-1}^{(S)})_2] =$$

$$= \left| \sum_{j=b\_mod\_i-1}^{b\_mod\_i+\Delta_{min}-2} 2^j x_j^{(S)} - 2^{b\_mod\_i+\Delta_{min}-1} x_{b\_mod\_i+\Delta_{min}-1}^{(S)} \right|_{m_i} =$$

$$= \left| \sum_{j=b\_mod\_i-1}^{b\_mod\_i+\Delta_{min}-2} W_{j,i} x_j^{(S)} - W_{b\_mod\_i+\Delta_{min}-1,i} x_{b\_mod\_i+\Delta_{min}-1}^{(S)} \right|_{m_i}.$$

_ПМ_РС.6В. Найти сумму $\chi_i = X_0^{(S)} + X_1^{(S)}$.

_ПМ_РС.6Г. При $\chi_i \geq m_i$ положить $\chi_i := \chi_i - m_i$.

_ПМ_РС.7. Если $i \neq k$, то инкрементировать переменную i (i:=i+1) и перейти к _ПМ_РС.2.

_ПМ_РС.8. Завершить работу алгоритма.

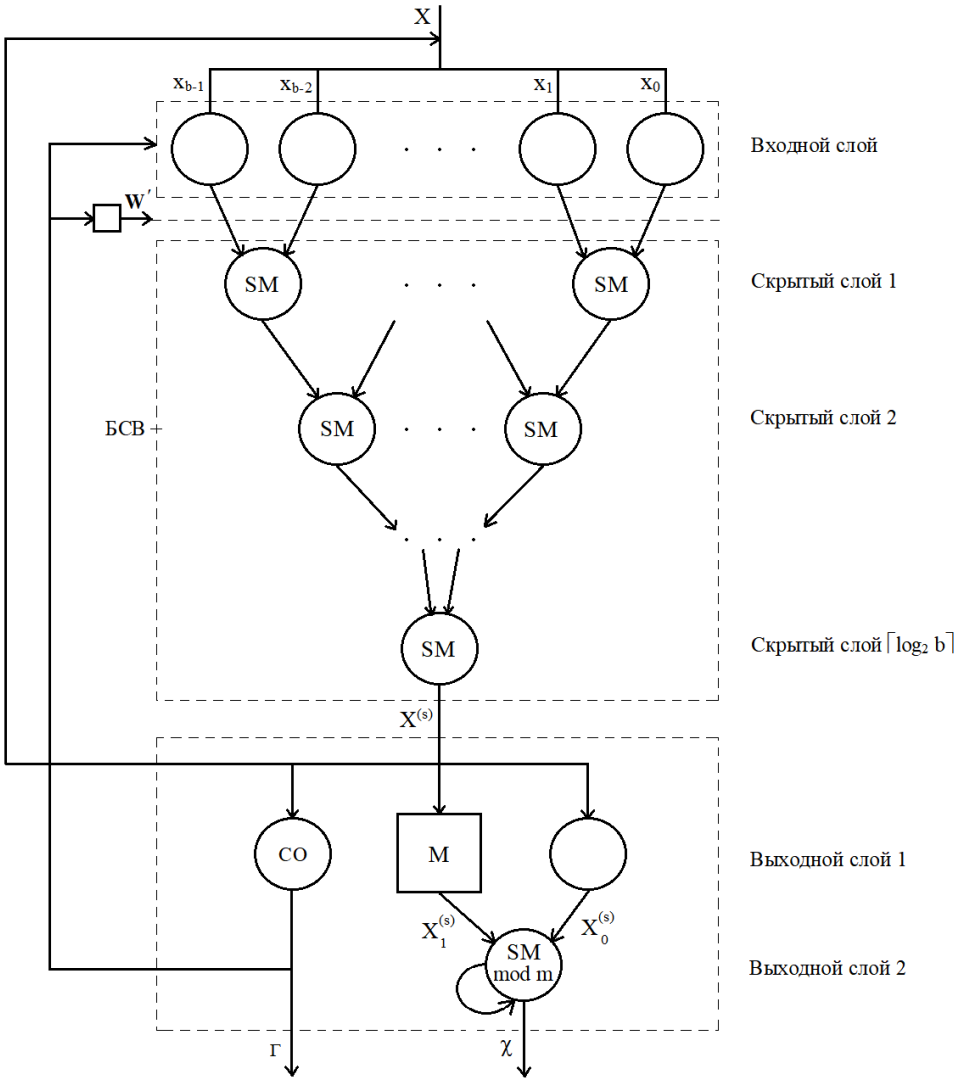
Нейросетевая реализация редукционного алгоритма позиционно-модулярного преобразования масштабируемых чисел. Синтезированная процедура _ПМ_РС.1–_ПМ_РС.8 приведения масштабируемых ЦЧ к остаткам по модулям $m \in \mathbf{M}=\{m_1, m_2, \dots, m_k\}$ ($k \geq 1$) может быть реализована как программно, так и аппаратным способом с применением нейросетевой вычислительной технологии [1, 3, 14, 15].

На рисунке изображена структура параллельной НСКК с обратной связью. Данная НС содержит входной слой, нейроны которого образуют b-разрядный регистр для фиксации двоичного кода $(x_{b-1} \; x_{b-2} \; x_0)_2$ ЦЧ X, $\lceil \log_2 b \rceil$ скрытых слоев, в совокупности составляющих блок суммирования вычетов – взвешенных компонент наборов вида (17), (18):

$$\mathbf{W}(C) = \left\{ W_j(C) \middle| W_j(C) = \left| C \;\; 2^j \right|_m^- ; j = \overline{0, b-1} \right\}; \tag{20}$$

$$\mathbf{W} = \left\{ W_j \middle| W_j = \left| 2^j \right|_m^- ; j = \overline{0, b_1 - 1} ; b_1 < b \right\}, \tag{21}$$

а также два выходных слоя, осуществляющих проверку принадлежности получаемых блоком суммирования вычетов (БСВ) чисел $X^{(s)} = (x_{b_s-1}^{(s)} \; x_{b_s-2}^{(s)} \; \dots \; x_0^{(s)})_2$ $(s = \overline{1, S})$ к диапазону $\mathbf{Z}_{b\_mod+\Delta_{min}}^-$ и приведение ЦЧ $X^{(S)}$ к остатку по модулю m.



Параллельная НСКК с обратной связью для позиционно-модулярного преобразования по рекурсивной редукционной схеме

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 вычетов, то вычет, не вошедший в пару, подвергается задержке на время сложения пар вычетов в данном слое. Обладая параллельной $\lceil \log_2 b \rceil$-каскадной «пирамидальной» архитектурой, БСВ формирует дополнительный двоичный код ЦЧ конвейерного типа. Это обеспечивает получение на выходе БСВ двоичного кода ЦЧ $X^{(s)}$ (см. (3)) за время $\lceil \log_2 b \rceil t_{сл}$, где $t_{сл}$ – длительность операции сложения двух вычетов.

Изображенная на рисунке НСКК работает следующим образом. Двоичный код $(x_{b-1}\ x_{b-2}\ \ldots\ x_0)_2$ ЦЧ X, подлежащего преобразованию $X \to |CX|_m$, фиксируется в нейронах входного слоя, откуда вместе с набором (20) синаптических весов поступает затем в БСВ. Реализуя рекурсивную $\lceil \log_2 b \rceil$-каскадную процедуру суммирования аддитивных компонент выражения для $X^{(1)}$ (см. (3)) 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 $\left(x_{b_1-1}^{(1)}\ x_{b_1-2}^{(1)} \ldots x_0^{(1)}\right)_2$ числа $X^{(1)}$. Старшая $(\Delta' + 1)$-битовая часть $\left(x_{b_1-1}^{(1)}\ x_{b_1-2}^{(1)} \ldots x_{b_1-\Delta'-1}^{(1)}\right)_2$ $(\Delta' = b_1 - b\_mod - \Delta_{min})$ сформированного кода подается в управляющий элемент *СО* первого выходного слоя, который в соответствии с булевым выражением (10), рассматриваемым при s=1, генерирует сигнал Δ. Единичное значение сигнала Δ указы-

вает на то, что ЦЧ, полученное на выходе БСВ, находится за пределами диапазона $\mathbf{Z}^{-}_{b\_mod+\Delta_{min}}$. В этом случае $\Delta = 1$ инициирует включение в НСКК обратной связи, что обеспечивает переход к очередной итерации редукционного процесса (3). Двоичный код с выхода БСВ передается во входной слой и согласно правилу

$$\mathbf{W}' = \begin{cases} \mathbf{W}(C), \text{если } \Gamma = 0, \\ \mathbf{W}, \text{если } \Gamma = 1, \end{cases}$$

набор **W** (*C*) синаптических весов замещается набором **W** (см. (21)). В результате на выходе БСВ сформируется двоичный код очередного элемента последовательности вычетов $X^{(1)}, X^{(2)}, \ldots, X^{(S)}$.

Функционирование НСКК в рекурсивном режиме завершается с появлением на выходе БСВ в рамках заключительной *S*-й итерации двоичного кода $(x^{(S)}_{b_S-1}\ x^{(S)}_{b_S-2}\ \ldots\ x^{(S)}_0)_2$ ЦЧ $X^{(S)}$ из диапазона $\mathbf{Z}^{-}_{2^{b\_mod+\Delta_{min}}}$. В данном случае сигнал Г, генерируемый управляющим элементом *CO*, принимает значение Г=0, что приводит к блокировке обратной связи. При этом извлекаемый из табличной памяти *M* первого выходного слоя по адресу $(x^{(S)}_{b\_mod+\Delta_{min}-1}\ x^{(S)}_{b\_mod+\Delta_{min}-2}\ \ldots\ x^{(S)}_{b\_mod-1})_2$ вычет $X^{(S)}_1$ вместе с сохраняемым в регистре вычетом $X^{(S)}_0$ (см. (14)–(16)) подаются на входы сумматора *SMmod m* второго выходного слоя, который в соответствии с (13) получает искомый остаток: $\chi = |CX|_m = \left|X^{(S)}\right|_m$.

Отметим, что значение параметра Δ_{min} можно регулировать, поэтому описанная конфигурация НСКК с обратной связью позволяет гибко устанавливать оптимальный баланс между количеством итераций применяемой редукционной схемы и объемом используемой табличной памяти.

Заключение. В статье представлены наиболее важные результаты разработки по созданию базовых НСКК для высокопроизводительных МА-приложений в области защиты информации.

Для построения НС на кольцах вычетов по модулям МСС как основы нейросетевого обеспечения криптографических МА-приложений использована редукционная технология позиционно-модулярного преобразования масштабируемых чисел. Развиваемые подходы к решению поставленной задачи обеспечивают оптимальные условия для согласования и реализации фундаментальных свойств параллелизма НС и МА. При этом для повышения скорости сходимости базовой рекурсивной вычислительной схемы применен табличный метод сокращения количества необходимых итераций.

Синтезирован новый эффективный алгоритм ускоренного преобразования масштабируемых чисел из двоичной системы в модулярную систему счисления по редукционной схеме понижения разрядности элементов формируемой последовательности вычетов. Благодаря применению гибкого адаптивного механизма проверки принадлежности поитерационных вычетов к специально выбираемому диапазону, допускающему табличную декомпозицию его элементов на пары компонент – остатков по модулям заданного базиса, реализуемый метод позволяет достичь значительного повышения скорости осуществляемого преобразования.

Разработана параллельная структура НСКК с обратной связью, выполняющей позиционно-модулярное преобразование масштабируемого целого числа по редукционной схеме за минимизированное количество S итераций – суммарное время $(S(\lceil \log_2 b \rceil + 1) + 2)t_{\text{сл}}$, где b – разрядность входного числа, $t_{\text{сл}}$ – длительность операции сложения двух вычетов.

Список использованных источников

1. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях / Н. И. Червяков [и др.]. – М. : Физматлит, 2017. – 400 с.

2. Ananda Mohan, P. V. Residue Number Systems: Theory and Applications / P. V. Ananda Mohan. – Basel : Birghauser, Mathematics, 2016. – 351 p.

3. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Н. И. Червяков [и др.]. – М. : Физматлит, 2012. – 280 с.

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

5. Omandi, A. Residue Number Systems: Theory and Implementation / A. Omandi, B. Premkumar. – Singapore : Imperial College Press, 2007. – 311 p.

6. Оцоков, Ш. А. Способ организации высокоточных вычислений в модулярной арифметике / Ш. А. Оцоков // Первая Междунар. конф. «Параллельная компьютерная алгебра и ее приложения в новых инфокоммуникационных системах». – Ставрополь, 20–24 окт., 2014. – Ставрополь : ИИЦ «Фабула», 2014. – С. 270–277.

7. Fast modular network implementation support vector machines / G.-B. Gulang [et al.] // IEEE Trans. Neural Networks. – 2005. – Vol. 16, no. 6. – P. 1651–1663.

8. Тихонов, Э. Е. Программно-аппаратная реализация нейронных сетей : моногр. / Э. Е. Тихонов, А. А. Евдокимов. – Невинномысск : НИЭУП, 2013. – 116 с.

9. Sanches, D. Optimization of modular granular neural networks using arhierarchical genetic algorithm based on the database comlexcity applied to human recognition / D. Sanches, P. Melin, O. Castillo // Informations Sciences. Tjuana Institute of Technology. – 2015. – Vol. 309. – P. 73–101.

10. Кондрашев, А. В. Нейронная сеть для преобразования чисел, представленных в позиционном коде, в систему остаточных классов [Электронный ресурс] / А. В. Кондрашев, Д. В. Горденко, Д. Н. Павлюк // Исследования в области естественных наук. – 2015. – № 1. – Режим доступа: http://science.snauka.ru/2015/01/8925. – Дата доступа: 22.01.2018.

11. Разработка нового нейросетевого метода вычисления модульного умножения в системе остаточных классов / М. Г. Бабенко [и др.] // Нейрокомпьютеры: разработка и применение. – 2016. – № 10. – С. 41–48.

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

13. Чернявский, А. Ф. Преобразование кода модулярной системы счисления в обобщенный позиционный код / А. Ф. Чернявский, А. А. Коляда // Доклады Нац. акад. наук Беларуси. – 2017. – Т. 61, № 4. – С. 26–30.

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

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

References

1. Chervjakov N. I., Koljada A. A., Ljahov P. A., Babenko M. G., Lavrinenko I. N., Lavrinenko A. V. 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., Evdokimov A. A., Galushkin A. I., Lavrinenko I. N., Lavrinenko A. V. 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. Omandi A., Premkumar B. *Residue Number Systems: Theory and Implementation*. Singapore, Imperial College Press, 2007, 311 p.

6. Ocokov Sh. A. Sposob organizatsii vysokotochnykh vychislenij v modulyarnoj arifmetike [The way to organize high-precision calculations in modular arithmetic]. Pervaja Mezhdunar. konf. «Parallel'naja komp'juternaja algebra i ee prilozhenija v novyh infokommunikacionnyh sistemah» [*First International Conf. "Parallel Computer Algebra and Its Applications in New Infocommunication Systems"*]. Stavropol, 20–24 Okt., 2014. Stavropol, Fabula Publ., 2014, pp. 270–277 (in Russian).

7. 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.

8. Tihonov Je. E., Evdokimov A. A. Programmno-apparatnaja realizacija nejronnyh setej : monografija. *Software and Hardware Implementation of Neural Networks*. Nevinnomyssk, NIJeUP Publ., 2013, 116 p. (in Russian).

9. Sanches D., 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, pp. 73–101.

10. Kondrashjov A. V., Gordenko D. V., Pavljuk D. N. Nejronnaya set' dlya preobrazovaniya chisel, predstavlennykh v pozitsionnom kode, v sistemu ostatochnykh klassov [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 (in Russian). Available at: http://science.snauka.ru/2015/01/8925 (accessed 22.01.2018).

11. Babenko M. G., Chernyh A. N., Kuchukov V. A., Derjabin M. A., Kuchukova N. N. Razrabotka novogo nejrosetevogo metoda vychisleniya modul'nogo umnozheniya v sisteme ostatochnykh klassov [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).

12. Koljada A. A. Obobshhennaya integral'no-kharakteristicheskaya baza modulyarnykh sistem schisleniya [Generalized integral-characteristic base of modular number systems]. Informacionnye tehnologii [*Information Technology*], 2017, vol. 23, no. 9, pp. 641–649 (in Russian).

13. Chernjavskij A. F., Koljada A. A. Preobrazovanie koda modulyarnoj sistemy schisleniya v obobshhennyj pozitsionnyj kod [Conversion of a modular number system code to a generalized positional code]. Doklady Natsional'noi akademii nauk Belarusi [*Doklady of the National Academy of Sciences of Belarus*], 2017, vol. 61, no. 4, pp. 26–30 (in Russian).

14. Chervjakov N. I., Evdokimov A. A. Nejronnye seti konechnogo kol'tsa dlya realizatsii porogovykh skhem razdeleniya sekreta [Neural networks of the finite ring for the implementation of threshold separation schemes for secretion]. Nejrokomp'jutery: razrabotka, primenenie [*Neurocomputers: Development and Application*], 2007, no. 2–3, pp. 45–50 (in Russian).

15. Chervjakov N. I., Spel'nikov A. B., Mezenceva A. F. Nejronnaya set' konechnogo kol'tsa pryamogo rasprostraneniya dlya operatsij na ehllipticheskikh krivykh [Neural network of a finite ring of direct propagation for operations on elliptic curves]. Nejrokomp'jutery: razrabotka, primenenie [*Neurocomputers: Development and Application*], 2008, no. 1–2, pp. 28–34 (in Russian).

Информация об авторах

Червяков Николай Иванович – доктор технических наук, профессор, Северо-Кавказский федеральный университет (пр. Кулакова, 2, 355029, Ставрополь, Российская Федерация). E-mail: Chervyakov@yandex.ru

Коляда Андрей Алексеевич – доктор физико-математических наук, доцент, главный научный сотрудник лаборатории специализированных вычислительных систем, Научно-исследовательское учреждение «Институт прикладных физических проблем им. А. Н. Севченко» Белорусского государственного университета (ул. Курчатова, 7, 220045, Минск, Республика Беларусь). E-mail: razan@tut.by

Коляда Назар Андреевич – научный сотрудник лаборатории специализированных вычислительных систем, Научно-исследовательское учреждение «Институт прикладных физических проблем им. А. Н. Севченко» Белорусского государственного университета (ул. Курчатова, 7, 220045, Минск, Республика Беларусь). E-mail: razan@tut.by

Кучуков Виктор Андреевич – специалист-патентовед отдела научно-технической информации, наукометрии и экспортного контроля, профессор, Северо-Кавказский федеральный университет (пр. Кулакова, 2, 355029, Ставрополь, Российская Федерация). E-mail: patentncfu@yandex.ru

Протасеня Стелла Юрьевна – младший научный сотрудник лаборатории специализированных вычислительных систем, Научно-исследовательское учреждение «Институт прикладных физических проблем им. А. Н. Севченко» Белорусского государственного университета (ул. Курчатова, 7, 220064, Минск, Республика Беларусь). E-mail: Estellita@mail.ru

Information about the authors

Nikolai I. Chervyakov – D. Sc. (Engineering), Professor, North-Caucasus Federal University (2, Kulakova Ave., 355029, Stavropol, Russian Federation). E-mail: Chervyakov@ yandex.ru

Andrey A. Kolyada – D. Sc. (Physics and Mathematics), Chief Researcher of the Laboratory of Specialized Computational Systems, Scientific Research Institution "Institute of Applied Physical Problems named after A. N. Sevchenko" of the Belarusian State University (7, Kurchatov Str., 220045, Minsk, Republic of Belarus). E-mail: razan@tut.by

Nazar A. Kolyada – Researcher, Laboratory of Specialized Computing Systems, Scientific Research Institution "Institute of Applied Physical Problems named after A. N. Sevchenko" of the Belarusian State University (7, Kurchatov Str., 220045, Minsk, Republic of Belarus). E-mail: razan@tut.by

Victor A. Kuchukov – Patent Holder of the Department of Scientific and Technical Information, Sciencemetry and Export Control, Professor, North-Caucasus Federal University (2, Kulakova Ave., 355029, Stavropol, Russian Federation).

E-mail: patentncfu@ yandex.ru

Stella Y. Protasenia – Junior Scientific Employee, Laboratory of Specialized Computational Systems, Scientific Research Institution "Institute of Applied Physical Problems named after A. N. Sevchenko" of the Belarusian State University (7, Kurchatov Str., 220064, Minsk, Republic of Belarus). E-mail: Estellita@mail.ru