УДК 681.04

МЕТОД КОРРЕКЦИИ ОШИБОК В СИСТЕМЕ ОБРАБОТКИ ЦИФРОВОЙ ИНФОРМАЦИИ, ФУНКЦИОНИРУЮЩЕЙ В МОДУЛЯРНОЙ АРИФМЕТИКЕ

ХЕРИ АЛИ АБДУЛЛАХ, В.А. КРАСНОБАЕВ, А.А. ЗАМУЛА, Ж.В. ДЕЙНЕКО, О.В. ЗЕФИРОВА

В статье рассматривается и предлагается к практическому использованию метод коррекции ошибок в непозиционной системе счисления – в модулярной арифметике. Данный метод целесообразно применять в криптографических системах обработки цифровой информации, функционирующих в реальном времени.

The paper considers and proposes to practical use a method of correcting errors in the nonposition numbering system – in modular arithmetic. It is expedient to use the said method in cryptographic systems of digital information processing functioning in real time.

ВВЕДЕНИЕ

Современный этап развития науки и техники отличается всё более сложными задачами, которые требуют своего решения. Однако сложность решаемых задач опережает темпы нарастания мощности универсальных ЭВМ. В этом аспекте, основными направлениями совершенствования систем обработки информации (СОИ), функционирующих в реальном времени, является повышения пользовательской производительности и безотказности функционирования, за счет обеспечения необходимого (заданного) уровня отказоустойчивости. Неуклонный рост объёмов информационных потоков циркулирующих в современных криптографических СОИ наряду с ужесточением требований по работе в реальном времени, жестко ставят проблему обеспечения выполнения криптографических преобразований большой размерности. Такие задачи способны решать, как правило, только вычислительные системы с высоким параллелизмом обработки информации. В качестве таких систем могут найти применение СОИ, функционирующие в непозиционной системе счисления – в модулярной арифметике (МА) [1-3].

Основания МА m_1, ..., m_n, будем называть информационными, а основания m_{n+1}, ..., m_{n+k} – контрольными. Если МА упорядочена, то $d_{\min} = k+1$, если МА расширяется путём добавления k оснований и каждое основание больше любого информационного основания, то минимальное расстояние кода автоматически увеличивается на величину k. Увеличить $d_{\min}$ можно также за счёт уменьшения числа информационных оснований, то есть, переходя к вычислениям с меньшей точностью. Таким образом, между корректирующими возможностями R – кодов и точностью вычислений существует обратно пропорциональная зависимость. Один и тот же вычислитель может выполнять арифметические операции с высокой точностью, но небольшой надежностью или с меньшей точностью, но с более высокой надежностью и скоростью (быстродействие выполнения основных операций в МА обратно пропорционально числу информационных оснований) [1, 4, 5].

Рассмотрим метод обнаружения ошибок в МА. Пусть задана МА основаниями m_1, m_2,..., m_n. Рабочий диапазон представления операндов определится $M = \prod_{i=1}^{n} m_i$. Введём ещё одно основание $m_{n+1} > m_n$, взаимно простое с любым из информационных оснований. В этом случае полный диапазон МА определиться как $M_1 = M \cdot m_{n+1}$. Рассмотрим результаты известных теорем.

Теорема 5.1. Если система остаточных классов упорядочена, то число $\tilde{A} = (a_1, a_2, ..., \tilde{a}_i \neq a_i, ..., a_{n+1})$ является неправильным, если число $\tilde{A} = (a_1, a_2, ..., a_i, ..., a_{n+1})$ правильное. Таким образом, чтобы обнаружить факт искажения числа $\tilde{A} = (a_1, a_2, ..., a_n, ..., a_{n+1})$, необходимо сравнить его с рабочим диапазоном М.

Если $A \geq M$, то число искажено, а если $A < M$, то либо ошибок нет, либо она носит более сложный характер. Рассмотрим алгоритм исправления ошибок. Введём ещё одно контрольное основание $m_{n+2} > m_{n+1}$. В этом случае полный диапазон МА определится так: $M_2 = M_1 \cdot m_{n+2}$. В этом случае алгоритм определения и исправления ошибочного остатка в СОК представится следующим образом [1, 3].

1. Вычисляются проекции числа

$$\tilde{A} = (a_1, a_2, ..., a_n, a_{n+1}, a_{n+2})$$

по всем основаниям МА:

$$\tilde{A}_1 = (a_2, a_3, ..., a_n, a_{n+1}, a_{n+2}),$$

$$\tilde{A}_2 = (a_1, a_3, ..., a_n, a_{n+1}, a_{n+2}),$$

$$\tilde{A}_{n+1} = (a_1, a_2, ..., a_n, a_{n+2}),$$

$$\tilde{A}_{n+2} = (a_1, a_2, ..., a_n, a_{n+1}).$$

2. Полученные проекции $\tilde{A}_i \left(i = \overline{1, n+2}\right)$ сравниваются с рабочим диапазоном M.

3. Определяя проекцию числа, для которой $\tilde{A}_i < M$, определяем ошибочный остаток по формуле:

$$a_i = \tilde{a}_i + \left[\frac{m_i \left(1 + j \cdot m_{n+1}\right)}{m_{n+1} \cdot \overline{m_i}} - \frac{\tilde{A}}{B_i} \right],$$

где: $B_i = \overline{m_i} \cdot M / m_i$ – ортогональный базис МА; $j = 0, 1, 2, ...$; $\overline{m_i}$ – вес ортогонального базиса.

Из характера рассмотренного кода видна его полная арифметичность – введенные основания включены в общую систему оснований МА и коды, содержащие цифры по всем как основным, так и контрольным разрядам, равнозначно участвуют в проведении любой операции; обработка основных и дополнительных цифр производится совершенно одинаковым образом, без какого-либо различия. Это позволяет считать, что обработка информации в МА может вестись без контроля каждого отдельного кода, а поэтапно. Величина (длина) каждого этапа определяется в каждом отдельном случае, либо по законченному циклу обработки массива информации, либо в соответствии с вероятностью возникновения одиночной ошибки. Конечный результат вычислений каждого этапа, может быть подвергнут контролю и его правильность подтверждает правильность проведения всех операций данного этапа. Отметим, что введение только одного контрольного основания позволяет обнаружить не только любую одиночную ошибку (как и в позиционных системах счисления (ПСС)), но и (в среднем) большую часть двойных.

Известно [6-8], что отличительной особенностью МА, является резкое проявление первичной информационной избыточности при введении вторичной $Q(l)$ информационной избыточности (за счёт наличия контрольных оснований МА, то есть $Q(l)=\prod_{j=1}^{l} m_{z\cdot j}$). Покажем, что код МА (в некоторых случаях) может обнаруживать некоторое число ошибок более высокой кратности, чем та, которая допускается в соответствии с общей теорией кодирования.

Пусть для МА минимальное кодовое расстояние определяется значением $d_{\min}$. Предположим, что в МА имеются такие основания, число которых $l \ge d_{\min}$ и при этом выполняется условие

$$Q(l)=\prod_{j=1}^{l} m_{z_j} < R = M_1 / M \ ,$$

когда у вектора ошибки $\Delta A = \tilde{A} - A$ должно быть не менее n-l нулевых компонент. Представим вектор ΔA в виде:

$$\Delta A = \left(0, Q, ..., \Delta a_{z_1}, ..., 0, \Delta a_{z_1}, 0\right).$$

В позиционной системе счисления имеем:

$$\Delta A = B_{z1}\cdot a_{z1} + ... + B_{zl}\cdot a_{zl} \ .$$

Учитывая, что $B_{zl} = \bar{m}_{zl}\cdot M_1 / m_{zl}$, где $\bar{m}_{zl}$ – вес l-го ортогонального базиса, запишем:

$$\Delta A = \frac{\bar{m}_{z1}\cdot M_1}{m_{z1}} a_{z1} + ... + \frac{\bar{m}_{zl}\cdot M_1}{m_{zl}} a_{zl} = R\cdot\Delta R\cdot Z \ , \quad (1)$$

$$\text{и} \ \ R\cdot\Delta R = \frac{M_1}{Q(l)}, \qquad Z = \sum_{j=1}^{l} \bar{m}_{zj}\cdot Q_j(l) \ .$$

$$Q_j(l) = \frac{Q(l)}{m_{zj}} \quad \left(M_1 = R\cdot\Delta R\cdot Q_j(l)\cdot m_{zj}\right).$$

Из выражения (1) очевидно, что

$$\Delta A \equiv 0 (\text{mod}\ M_1 / Q(l)) \ .$$

Тогда имеем:

$$\Delta A / Z_0 = R\cdot\Delta R = M_1 / Q(l) \ge M_l / R = M \ , \qquad (2)$$

где $Z_0 = 1, 2, ...$ Из (2) следует, что $\Delta A \ge M$ и, таким образом,

$$\tilde{A} = A + \Delta A > M \ . \qquad (3)$$

Неравенство (3) показывает, что сумма любого числа А и числа, соответствующего вектору ошибки ΔA, не может принадлежать множеству M, то есть, подобную ошибку можно обнаружить. Отметим, что даже в тех случаях, когда $Q(l) > R$, среди ошибок ΔA найдутся такие, которые удовлетворяют неравенству (3). Это возможно за счёт наличия вторичной информационной избыточности ΔR .

Специфика представления чисел в МА позволяет в ряде случаев не только обнаружить ошибку, но и найти место её возникновения, используя только одно контрольное основание, что невозможно при существующих методах контроля и коррекции в ПСС, например, при контроле по модулю. Осуществить коррекцию ошибок при $d_{\min} = 2$ можно либо способом проекций, либо используя понятие альтернативной совокупности (АС). Способ проекций требует вычислений всех проекций $\tilde{A}_i$ искаженного числа, что ведет к выполнению большего количества операций при каждой коррекции результата. Аппаратурная и особенно программная реализация способа проекций приводит к большим затратам времени. Кроме того, этот способ принципиально не позволяет однозначно обнаружить место возникновения любых одиночных ошибок.

Значительно большей эффективностью обладает разработанный и предлагаемый в данной статье метод альтернативной совокупности чисел в МА.

ОСНОВНАЯ ЧАСТЬ

Метод повышения информативности альтернативной совокупности чисел в МА

Замечательной особенностью МА является возможность коррекции ошибок даже при наличии только одного контрольного основания, используя понятие альтернативной совокупности чисел.

Совокупность оснований m_{i1}, m_{i2},..., m_{ik}, по которым числа A_1, A_2, ..., A_k отличаются от неправильного числа $\tilde{A}$, будем называть альтернативной совокупностью числа $\tilde{A}$ и обозначать $W(\tilde{A}) = \{m_{i1}, m_{i2}, \ldots, m_{ik}\}$.

Основной принцип определения ошибочного остатка $\tilde{a}_i$ состоит в том, что для получаемой в результате операций, последовательности неправильных операндов $\tilde{A}_1, \tilde{A}_2, ..., \tilde{A}_\rho$ в процессе выполнения программы последовательно во времени определяются условные альтернативные совокупности (УАС) вида:

$$W(\tilde{A}) = W(\tilde{A}_1) \wedge W(\tilde{A}_2) \wedge \ldots \wedge W(\tilde{A}_\rho),$$

где $W(\tilde{A}_l) = \{m_{q1}, m_{q2}, \ldots, m_{qk}\}$ – альтернативная совокупность l –го неправильного числа.

Определим время коррекции ошибок в динамике вычислительного процесса. Известно, что общее время коррекции ошибок равно

$$T_{\text{корр}} = T_{\text{об}} + T_{\text{исп}}.$$

Для МА время обнаружения ошибок в динамике вычислительного процесса определяется как:

$$T_{\text{об}} = K_1 \cdot T_{\text{пр}\gamma_{n+1}} + K_2 \cdot T_{\text{прАС}} + K_3 \cdot T_{\text{прУАС}},$$

где $T_{\text{пр}\gamma_{n+1}} = T_{\text{н}} + T_{\gamma_{n+1}}$ – время определения и проверки значения γ_{n+1}; $T_{\text{прАС}} = T_{\text{опрАС}} + T_{\text{опр}W(\tilde{A})}$ – время определения и проверки АС; $T_{\text{прУАС}} = T_{\text{опрУАС}} + T_{W\wedge(\tilde{A})}$ – время определения и проверки УАС; K_1, K_2, K_3 – коэффициенты кратности определения соответственно операции нулевизации $(\tilde{A}^{(H)})$, операции определения альтернативной совокупности чисел $(W(\tilde{A}))$ и определения условной альтернативной совокупности чисел $(W \wedge (\tilde{A}))$.

Таким образом, время коррекции ошибок в динамике вычислительного процесса СОИ в МА определится следующим выражением:

$$T_{\text{корр}} = K_1\left(T_{\text{н}} + T_{\gamma_{n+1}}\right) + K_2\left(T_{\text{опрАС}} + T_{\text{опр}W(\tilde{A})}\right) + K_3\left(T_{\text{опрУАС}} + T_{W\wedge(\tilde{A})}\right) + T_{\text{исп}}.$$

Отметим, что если число A не искажено, то $K_1 = 1$, $K_3 = 0$, то есть

$$T_{\text{корр}} = T_{\text{об}} = T_{\text{н}} + T_{\gamma_{n+1}}.$$

Учитывая то, что операции определения АС, УАС и исправление ошибок в МА могут выполняться в табличном варианте, то есть в один такт, то получим $T_{\text{корр}} \approx k \cdot T_{\text{н}}$ (4).

Исходя из последнего соотношения, очевидны два основных пути уменьшения времени $T_{\text{корр}}$ коррекции ошибок. Первый путь заключается в уменьшении количества этапов K определения АС. Это достигается за счет применения разработанных в [1, 3] методов коррекции ошибок в МА. Второй путь состоит в уменьшении времени нулевизации $T_{\text{н}}$. Это достигается за счёт применения метода парной нулевизации с предварительной выборкой цифр [3]. При коррекции ошибок в динамике вычислительного процесса предполагается, что реализуемая цепь операций обладает достаточной длиной, позволяющей стянуть условные АС к ошибочному основанию.

Возможны три варианта коррекции ошибок.

1. В ходе вычислений последовательно определяются УАС, и за время $\Delta t_{\text{ОПР\_ОШ}}$ стягиваются к ошибочному основанию.

2. По первой АС принимается определённая гипотеза, проводится коррекция результата до обнаружения факта ошибочности принятой гипотезы. В этом случае необходимо перейти на другую гипотезу.

3. Третий вариант состоит из синтеза первого и второго. Определяются УАС чисел, получающихся по мере реализации программы вычислений вплоть до стягивания их в числе $\tilde{A}$ к двум основаниям m_i и m_{n+1}. Далее принимается гипотеза ошибочности остатка $\tilde{a}_i$ и приводится коррекция. Если гипотеза окажется несостоятельной, то ошибочной цифрой будет $\tilde{a}_{n+1}$.

Таким образом, при любом существующем варианте коррекции ошибок в динамике вычислительного процесса возникает необходимость в определении АС, то есть эффективность любого из возможных вариантов коррекции ошибок зависит от метода определения альтернативной совокупности чисел.

Как правило, продолжительность цикла вычислений для данного алгоритма является величиной постоянной $t_k - t_H = const$, в связи с этим, необходимо стремиться к уменьшению времени $\Delta t_{\text{ОПР\_ОШ}}$. Это может достигаться следующими путями.

1. Создание в начале цикла вычислений утяжеленных режимов работы СОИ, что может привести к сдвигу временной оси влево к t_H. Иными словами, ошибка обнаруживается сразу после начала цикла вычислений. Однако этот путь не гарантирует высокую вероятность обнаружения ошибки в начале цикла вычислений.

2. Уменьшение времени $\sum_{i=1}^{k-1} \Delta t_{\text{ОСТ}V}$. Это можно достичь при «дроблении» операций на более короткие. Однако в большинстве случаев такое «дробление» операций либо невозможно, либо нецелесообразно.

3. Уменьшение времени $\sum_{i=1}^{k-1} \Delta t_{\wedge V}$. Это достигается за счёт ускорения процесса логического умножения $W(\tilde{A}_i) \wedge W(\tilde{A}_{i+1})$. Как правило, блок определения УАС строится по табличному принципу. В связи с этим, нет основания надеяться на то, что возможно существенное повышение быстродействия операции логического умножения.

4. Уменьшение времени $\sum_{i=1}^{k} \Delta t_{\text{АС}V}$. Это можно достичь за счёт повышения быстродействия операции нулевизации. В [3] показано, что время нулевизации можно (в зависимости от длины машинного слова) сократить на (20-25)% .

5. Уменьшение количества проверяемых операндов K (количество этапов определения АС). Это достигается за счёт повышения информативности (уменьшение в АС количества оснований, по которым возможна ошибка) $W(\tilde{A})$.

В связи с вышеизложенным материалом, необходимы и актуальны исследования, посвященные разработке эффективных методов определения АС, позволяющие повысить информативность $W(\tilde{A})$.

Методы определения альтернативной совокупности АС $W(\tilde{A})$ чисел в МА

Предлагаются два метода определения АС $W(\tilde{A})$.

Первый метод состоит в том, что АС $W(\tilde{A})$ устанавливается проверкой каждого из оснований m_i ($i=\overline{1,n+1}$) следующим образом. Определяется последовательность чисел, имеющих одни и те же цифры по всем основаниям, что и число $\tilde{A}$, кроме основания m_ρ и отличающихся лишь цифрами по этому основанию, то есть чисел вида:

$$A_{\rho S}=\left(a_1,a_2,...,a_{\rho-1}Sa_{\rho+1},...,a_{n+1}\right), \qquad (5)$$

где $S=\overline{1,m_\rho-1}$. Среди чисел вида (5) может не быть ни одного правильного числа, либо может быть только одно правильное число. В последнем случае m_ρ входит в АС операнда $\tilde{A}$. Проведя аналогичные проверки для каждого из оснований МА, определим

$$W(\tilde{A})=\left\{m_z,m_{z2},...,m_{zk}\right\}.$$

Недостаток первого метода – большие аппаратные и временные затраты.

При втором методе операнд $\tilde{A}$ приводится к виду

$$\tilde{A}^{(H)}=(0,0,...,0,\gamma_{n+1}),$$

то есть производится нулевизация числа $\tilde{A}$. В соответствии с теоремой о распределении ошибок, номер (j + 1) интервала, в который попадает число, $\tilde{A}$ определяется формулой:

$$j=\left[\frac{\Delta a_i\cdot\bar{m}_i\cdot m_{n+1}}{m_i}\right](\mathrm{mod}\,m_{n+1})+\Delta_{\text{доб}}, \qquad (6)$$

где $\Delta_{\text{доб}}$ принимает значение 0 или 1; $[x]$ – является целой частью числа x, не превышающей x.

В соответствии с выражением (6) составляется таблица значений соответствий числа γ_{n+1} возможным ошибкам Δa_i, где

$$j=\gamma_{n+1}\cdot\bar{m}_{n+1}(\mathrm{mod}\,m_{n+1}).$$

Из таблицы соответствий определяется искомая АС:

$$W(\tilde{A})=\left\{m_{l1},m_{l2},...,m_{l\rho}\right\}.$$

Второй метод в сравнении с первым позволяет сократить аппаратурные и временные затраты при определении АС, однако, недостаток второго метода состоит в том, что в АС содержатся избыточные основания. Это обусловлено тем, что значениям γ_{n+1} соответствуют ошибки Δa_i, относящиеся не только к искаженному операнду $\tilde{A}$, а и к группе операндов $\tilde{A}_к$, лежащих в интервале $j\cdot\left[\frac{M_1}{m_{n+1}},(j+1)\cdot\frac{M_1}{m_{n+1}}\right]$, где $M_1=\prod_{i+1}^{n+1}m_i$. Содержащиеся в АС избыточные основания снижают информативность $W(\tilde{A})$. Действительно, с увеличением числа оснований возрастает энтропия обнаружения ошибки по одному из оснований МА. Повышение энтропии определения ошибочного основания m_i увеличивает количество проверяемых операндов K (циклов проверки), а это, в свою очередь, увеличивает время стягивания АС к ошибочному основанию. Данный метод не может быть эффективно применён в короткой цепи вычислений СОИ. Таким образом, возникает необходимость в разработке методов определения АС, посредством которых возможна эффективная коррекция ошибок в короткой цепи вычислений СОИ.

Метод повышения информативности альтернативной совокупности чисел в МА

Коротко рассмотрим метод повышения информативности АС в МА, основанный на получении дополнительной информации о возможных искаженных остатков неправильного операнда $\tilde{A}$. Эта информация содержится во всех возможных АС операнда $\tilde{A}$. Пусть задана СОК упорядоченными основаниями m_1, ...,m_{n+1} и пусть в цепи вычислений определено неправильное число $\tilde{A}$. С целью повышения информативности о местоположении и величине ошибки предлагается дополнительно определить АС числа вида:

$$W_{k\rho_i}\left(\tilde{A}\right)=\left\{m_{k1},m_{k1},...,m_{k\rho_i}\right\},$$

то есть совокупность АС:

$$W_{1\rho_1}\left(\tilde{A}\right)=\left\{m_{11},m_{12},...,m_{1\rho_1}\right\},$$

$$W_{2\rho_2}\left(\tilde{A}\right)=\left\{m_{21},m_{22},...,m_{2\rho_2}\right\} \qquad (7)$$

$$W_{n+1\rho_{n+1}}\left(\tilde{A}\right)=\left\{m_{n+11},m_{n+12},...,m_{n+1\rho_{n+1}}\right\}.$$

Чтобы определить совокупность значений (7), предварительно вычислим

$$j_k=\bar{m}_k\cdot\gamma_k(\mathrm{mod}\,m_k) \qquad (8)$$

для $K=1,2,...,n,n+1$. Отметим, что при $K=n+1$ $W_{n+1\rho_{n+1}}(\tilde{A})=W(\tilde{A})$. В соответствии с выражением (5.11) составляем K таблиц, где значениям γ_k сопоставляются значения Δa_i. После того, как определены АС $W_{k\rho i}(\tilde{A})$, которые назовём первичными, определим вторичные значения ошибок Δa_i:

$$W_1^{(1)}(\tilde{A})=\left\{\Delta a_1^{(1)},\Delta a_2^{(1)},...,\Delta a_{n+1}^{(1)}\right\},$$

$$W_1^{(\psi_1)}(\tilde{A})=\left\{\Delta a_1^{(\psi_1)},\Delta a_2^{(\psi_1)},...,\Delta a_{n+1}^{(\psi_1)}\right\},$$

$$W_2^{(2)}(\tilde{A})=\left\{\Delta a_1^{(2)},\Delta a_2^{(2)},...,\Delta a_{n+1}^{(2)}\right\},$$

$$W_2^{(\psi_2)}(\tilde{A})=\left\{\Delta a_1^{(\psi_2)},\Delta a_2^{(\psi_2)},...,\Delta a_{n+1}^{(\psi_2)}\right\},$$

и так далее до значения векторов

$$W_n^{(\psi_n)}(\tilde{A})=\left\{\Delta a_1^{(\psi_n)},\Delta a_2^{(\psi_n)},...,\Delta a_{n+1}^{(\psi_n)}\right\},$$

и

$$W_{n+1}(\tilde{A})=\left\{\Delta a_1,\Delta a_2,...,\Delta a_{n+1}\right\},$$

компоненты вектора $W_{n+1}(\tilde{A})$ сравниваются с соответствующими компонентами всех векторов $W_i^{(\psi_i)}(\tilde{A})$ для i = 1, 2, ..., n. В совпадающих по величине компонентах векторов определяются основания СОК, набор которых и определяет искомую (результирующую) АС

$$W'(\tilde{A}) = \{m_{z1}, m_{z2}, ..., m_{z\rho}\}.$$

Действительно, среди АС $W_{k\rho i}\left(\tilde{A}\right)$ всегда содержится основание m_i, по которому произошла ошибка Δa_i, и это основание может быть только среди оснований общих для совокупности (7), то есть:

$$W(\tilde{A}) \geq W'(\tilde{A}). \qquad (9)$$

Если Δa_i такое, что $\tilde{A} = A + \Delta A$ лежит в интервале $[(m_{n+1} - 1) \cdot M, M_1]$, то

$$W(\tilde{A}) = W'(\tilde{A}). \qquad (10)$$

ВЫВОДЫ

Таким образом, сущность предложенного метода заключается в том, что определяются все возможные АС на каждом из интервалов попадания операндов $\tilde{A}$. После этого определяются общие для этих интервалов основания m_{z1}, ..., m_{zp}, по которым возможна ошибка. Этот набор оснований и определяет искомую АС. Сохранение количества оснований в АС повышает информативность АС $W(\tilde{A})$ о месте и величине ошибки. Это уменьшает время стягивания АС к ошибочному основанию (уменьшается количество этапов определения УАС), что повышает эффективность корректирующих кодов в МА.

Литература.

[1] *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. М.: Сов. радио. – 1968. – 440 с.

[2] Материалы Международной научно-технической конференции «50 лет модулярной арифметике». МИЭТ, г. Зеленоград. Моск. обл. 23–25 ноября 2005г.

[3] *Жихарев В.Я., Илюшко Я.В., Кравець Л.Г., Краснобаев В.А.* Методы и средства обработки информации в непозиционной системе счисления в остаточных классах. – Житомир: Изд-во «Волынь», 2005. – 220 с.

[4] *Краснобаев В.А.* Методы реализации модульных операций в системах цифровой обработки информации // Радиотехника. 2001. Вып. 119. С. 130–134.

[5] *Илюшко В.М., Краснобаев В.А., Деренько Н.С., Илюшко Я.В., Khery A. Abdullah.* Методы реализации криптографических преобразований с открытым ключом на основе использования кодов модулярной арифметики // Радіоелектронні і комп'ютерні системи. – 2006. – №4 (16). – С. 31–39.

[6] *Краснобаев В.А., Деренько Н.С., Зефирова О.В.* Исследование влияния системы счисления на отказоустойчивость систем обработки цифровой информации // Праці Таврійської державної агротехнічної академії. Наукове фахове видання. Мелітополь. Вип. 43. 2006. С.11–19.

[7] *В.И. Барсов, В.А. Краснобаев, Khery A. Abdullah, О.В. Зефирова.* Концепция создания нейрокомпьютеров систем управления на основе использования модулярной арифметики // Радіоелектронні і комп'ютерні системи. – 2007. – № 6 (25). – С. 40–54.

[8] *В.А. Краснобаев, В.И. Барсов, Е.В. Яськова.* Отказоустойчивые вычислительные системы на основе модулярной арифметики: концепции, методы и средства // Радіоелектронні і комп'ютерні системи. – 2007. – № 8 (27). – С. 82–90.

Поступила в редколлегию 4.09.2008

Хери Али Абдуллах, аспирант кафедры производства радиоэлектронных средств летательных аппаратов Национального аэрокосмического университета им. Н.Е. Жуковского («ХАИ»). Область научных интересов: технология создания систем обработки информации летательных аппаратов на основе использования непозиционных кодовых структур модулярной арифметики.

Краснобаев Виктор Анатолиевич, профессор кафедры автоматизации и компьютерных технологий Харьковского национального технического университета сельского хозяйства им. Петра Василенко, доктор технических наук, профессор, Заслуженный изобретатель Украины, Почётный радист СССР. Область научных интересов: теоретическое обоснование и практическое создание сверхбыстродействующих и высокоотказоустойчивых вычислительных структур в модулярной арифметике.

Замула Александр Андреевич, профессор кафедры БИТ ХНУРЭ, кандидат технических наук, доцент. Область научных интересов: технологии защиты информации в информационно-телекоммуникационных системах.

Зефирова Ольга Владимировна, ассистент кафедры высшей математики Харьковского национального технического университета сельского хозяйства им. Петра Василенко.

Дейнеко Жанна Валентиновна, старший преподаватель факультета последипломного образования ХНУРЭ, соискатель кафедры информатики ХНУРЭ. Область научных интересов: математическое моделирование, изучение систем нелинейной динамики, построение фазовых портретов, проектирование многозначной логики.