УДК 004.052.2:629.783

ИСПОЛЬЗОВАНИЕ ИЗБЫТОЧНЫХ МОДУЛЯРНЫХ КОДОВ ПРИ РАЗРАБОТКЕ ОТКАЗОУСТОЙЧИВЫХ ЗАПРОСНО-ОТВЕТНЫХ СИСТЕМ РАСПОЗНАВАНИЯ СПУТНИКА

[1]Калмыков М.И., [2]Бабенко Л.К., [1]Калмыков И.А., [1]Ефременков И.Д., [1]Мирошников Д.А.

[1]ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru;

[2]ФГАОУ ВО «Южный федеральный университет», Ростов-на-Дону

В работе представлены новые принципы использования параллельных модулярных кодов при построении запросно-ответной системы распознавания спутника. Применение запросно-ответных систем в комплексах дистанционного контроля, мониторинга и управления позволяет повысить имитозащиту низкоорбитальной системы спутниковой связи (ССС). В результате их работы спутник-нарушитель, который находится в зоне видимости станции связи, расположенной на необслуживаемом объекте, не сможет навязать ретрансляционную помеху. Данная помеха, имитирующая команду управления, может вывести из строя объект контроля, что может привести к экологической катастрофе. Повысить эффективность работы запросно-ответной системы распознавания спутника можно за счет использования модулярных кодов. катастрофы. Независимая и параллельная обработка остатков по основаниям модулярного кода служит основой не только повышения скорости вычислений, но и надежности устройства. Целью исследований является повышение надежности запросно-ответных системы за счет использования разработанного алгоритма поиска и коррекции ошибок с помощью модулярных кодов.

Ключевые слова: запросно-ответные системы распознавания спутника, корректирующий модулярный код, позиционная характеристика, алгоритм обнаружения и коррекции ошибок

THE USE OF REDUNDANT MODULAR CODES IN THE DEVELOPMENT OF FAULT-TOLERANT REQUEST-RESPONSE RECOGNITION SYSTEMS SATELLITE

[1]Kalmykov M.I., [2]Babenko L.K., [1]Kalmykov I.A., [1]Efremenkov I.D., [1]Miroshnikov D.A.

[1]Federal State Autonomous Educational Institution Higher Professional Education «North-Caucasian Federal University», Stavropol, e-mail:kia762@yandex.ru;

[2]Federal State Autonomous Educational Institution of Higher Education «Southern Federal University», Rostov-on-Don

The paper presents new principles of request-response detection system of the satellite by using a parallel modular codes. The use of request-response systems to systems of remote control, monitoring and management allows you to increase Kitazawa low-orbit satellite communication system (SSS). As a result of their work, the satellite, the offender, who is within sight of the stations that located on unattended object will not be able to impose relay interference. This obstacle simulates the management team, will damage the test object, which can lead to environmental disaster. To improve the efficiency of the request-response detection system the satellite can be due to the use of modular codes. disaster. abate presents a mathematical model implementation of discrete wavelet transform with the use of modular codes. Independent and parallel processing of residues on the grounds modular code is the basis not only improve the computing speed but also the reliability of the device. The aim of the research is to improve the reliability of the request-response system through the use of the developed search algorithms and error correction using modular.

Keywords: request-response detection system of the satellite, correcting modular code, positional characteristics, the detection algorithm and error correction

В настоящее время низкоорбитальные системы спутниковой связи применяются в комплексах дистанционного контроля, мониторинга и управления необслуживаемыми объектами добычи и транспортировки углеводородов, расположенных на Крайнем Севере. С целью предотвращения навязывания активной имитационной помехи чужим спутником-нарушителем предлагается использовать запросно-ответные системы распознавания спутника (ЗОСРС). В работе [1] представлен способ построения ЗОСРС, который применяет протокол аутентификации типа «запрос-ответ», использующий доказательство с нулевым разглашением знаний. Так как все вычислительные операции проводятся по большому модулю, чтобы обеспечить высокую имитостойкость протокола, то запросно-ответная система распознавания спутника характеризуется значительными схемными затратами. Это негативно влияет на надежность работы ЗОСРС. Решить данную проблему можно за счет применения модулярных кодов (МК). Поэтому разработка новых принципов построения запросно-ответной системы распознавания спутника в модулярном коде является актуальной задачей.

Цель исследования

Использование модулярных кодов позволяет повысить точность и скорость выполнения операций сложения, вычитания и умножения по модулю [2, 3]. Переход к параллельной и независимой обработке данных, отсутствие обмена промежуточных результатов вычислений между основаниями МК служит основой для применения таких кодов в процедурах поиска и коррекции ошибок. В отличие от известных помехоустойчивых кодов модулярные коды могут исправлять ошибки, которые возникают в процессе выполнения арифметических операций, тем самым повышая надежность работы вычислительных устройств. Поэтому целью работы является повышение надежности запросно-ответных системы за счет использования разработанного алгоритма поиска и коррекции ошибок с помощью модулярных кодов.

Материалы и методы исследования

С целью повышения надежности запросно-ответной системы опознавания статуса спутника, способ построения которой представлен в работах [1, 4–6], предлагается использовать МК, в частности коды системы остаточных классов (СОК). Коды СОК относятся к непозиционным кодам, в которых число X представляется в виде кортежа остатков $(x_1, x_2, ..., x_k)$, где $X \equiv x_i \bmod m_i$; $i = 1,2,\ldots, k$. Взаимно простые числа m_i являются основаниями кода СОК. Их произведение определяет рабочий диапазон СОК

$$\text{М}_{\text{раб}} = \prod_{i=1}^{k} m_i. \quad (1)$$

Числа $X = (x_1, x_2, ..., x_k)$ и $Y = (y_1, y_2, ..., y_k)$, которые представлены в коде СОК, можно быстро и параллельно складывать, вычитать и умножать по модулям m_i. Тогда справедливо

$$X + Y = ((x_1 + y_1) \bmod m_1, (x_2 + y_2) \bmod m_2, ..., (x_k + y_k) \bmod m_k), \quad (2)$$

$$X - Y = ((x_1 - y_1) \bmod m_1, (x_2 - y_2) \bmod m_2, ..., (x_k - y_k) \bmod m_k), \quad (3)$$

$$X \cdot Y = ((x_1 \cdot y_1) \bmod m_1, (x_2 \cdot y_2) \bmod m_2, ..., (x_k \cdot y_k) \bmod m_k), \quad (4)$$

где $Y \equiv y_i \bmod m_i$; $i = 1,2,\ldots, k$.

Для разработки новых принципов построения запросно-ответной системы распознавания спутника в модулярном коде необходимо выбрать основания МК, которые бы имели одинаковый первообразный элемент g и удовлетворили условию

$$\text{М}_{\text{раб}} = \prod_{i=1}^{k} m_i > q, \quad (5)$$

где q – модуль, используемый в работе ЗОСРС; g – первообразный элемент мультипликативной группы, порожденной простым числом q.

Воспользуемся алгоритмом работы ЗОСРС, приведенным в работе [1]. Для повышения имитостойкости ЗОСРС в системе кроме секретного ключа U используется сеансовый ключ $S(j)$, а также параметр $T(j)$, который позволяет определить повторное применение сеансового ключа. Представим их в модулярном коде. Тогда

$$U = (u_1, u_2, ..., u_k);$$

$$S(j) = (S_1(j), S_2(j), ..., S_k(j));$$

$$T(j) = (T_1(j), T_2(j), ..., T_k(j)), \quad (6)$$

где

$$U \equiv u_i \bmod m_i; \; S(j) \equiv S_i(j) \bmod m_i;$$

$$T(j) \equiv T_i(j) \bmod m_i; \; i = 1, 2, \ldots, k.$$

На первом этапе ответчик определяет истинный статус спутника с использованием МК

$$\begin{cases} C_1 = \left| g^{u_1} g^{S_1(j)} g^{T_1(j)} \right|_{m_1}^{+} \\ \vdots \\ C_k = \left| g^{u_k} g^{S_k(j)} g^{T_k(j)} \right|_{m_k}^{+} \end{cases}. \quad (7)$$

На втором этапе ответчик производит зашумление модулярного кода согласно

$$u_i^* = \left| u_i + \Delta u_i \right|_{m_i}^{+};$$

$$S_i^*(j) = \left| S_i(j) + \Delta S_i(j) \right|_{m_i}^{+};$$

$$T_i^*(j) = \left| T_i(j) + \Delta T_i(j) \right|_{m_i}^{+}. \quad (8)$$

где

$$\Delta U \equiv \Delta u_i \bmod m_i; \; \Delta S(j) \equiv \Delta S_i(j) \bmod m_i;$$

$$\Delta T(j) \equiv \Delta T_i(j) \bmod m_i; \; i = 1, 2, \ldots, k.$$

На третьем этапе ответчик определяет зашумленный статус спутника в МК

$$\begin{cases} C_1^* = \left| g^{u_1^*} g^{S_1^*(j)} g^{T_1^*(j)} \right|_{m_1}^{+} \\ \vdots \\ C_k^* = \left| g^{u_k^*} g^{S_k^*(j)} g^{T_k^*(j)} \right|_{m_k}^{+} \end{cases}. \quad (9)$$

На четвертом этапе запросчик пересылает вопрос $d = (d_1, d_2, \ldots, d_k)$ ответчику.

На пятом этапе ответчик приступает к вычислению ответов на вопрос d, согласно

$$r_i(1) = \left| u_i^* - d_i u_i \right|_{\varphi(m_i)}^{+};$$

$$r_i(2) = \left| S_i^*(j) - d_i S_i(j) \right|_{\varphi(m_i)}^{+};$$

$$r_i(3) = \left| T_i^*(j) - d_i T_i(j) \right|_{\varphi(m_i)}^{+}. \quad (10)$$

На шестом этапе ответчик передает запросчику сигнал в виде

$$\left\{(C_1, C_2, ..., C_k), (C_1^*, C_2^*, ..., C_k^*), (r_1(1), r_2(1), ..., r_k(1)), (r_1(2), r_2(2), ..., r_k(2)), (r_1(3), r_2(3), ..., r_k(3))\right\}.$$

На седьмом этапе запросчик проверяет истинность полученных ответов

$$\begin{cases} Y_1 = \left|C_1^{d_1} g^{r_1(1)} g^{r_1(2)} g^{r_1(3)}\right|_{m_1}^{+} \\ \vdots \\ Y_k = \left|C_k^{d_k} g^{r_k(1)} g^{r_k(2)} g^{r_k(3)}\right|_{m_k}^{+} \end{cases}. \quad (11)$$

Спутник будет считаться «своим», если будет справедливо равенство

$$\left\{ Y_1 = C_1^*, Y_2 = C_2^*, ..., Y_k = C_k^*\right\}. \quad (12)$$

Чтобы выполнять поиск и исправление ошибок, необходимо в модулярный код ввести избыточные основания [5, 7, 8]. Для исправления однократной ошибки вводятся два основания m_{k+1}, m_{k+2}, которые удовлетворяют условию

$$m_{k+2} > m_{k+1} > m_k > ... > m_1. \quad (13)$$

Это приводит к появлению полного диапазона МК

$$\text{М}_{\text{полн}} = \prod_{i=1}^{k+2} m_i = \text{М}_{\text{раб}} m_{k+1} m_{k+2}. \quad (14)$$

Если кодовая комбинация МК не превышает значения $\text{М}_{\text{раб}}$, то такая комбинация не содержит ошибки. В противном случае – комбинация является запрещенной. Чтобы определить данное условие в МК используют позиционные характеристики (ПК) [2, 6, 7, 9]. В работе предлагается разработанный алгоритм вычисления интервальный номер числа. Известно

$$L = \left\lfloor A / \text{М}_{\text{раб}} \right\rfloor, \quad (15)$$

где $\lfloor\ \rfloor$ – целая частного, полученного от деления.

В алгоритме используется китайская теорема об остатках (КТО), согласно которой

$$X = \left|x_1 B_1 + x_2 B_2 + ... + x_{k+2} B_{k+2}\right|_{M_{\text{раб}}}^{+} = \left|\sum_{i=1}^{k+2} x_i B_i\right|_{M_{\text{раб}}}^{+}, \quad (16)$$

где B_i – ортогональный базис основания m_i.

Для вычисления L воспользуемся свойством подобия ортогональных базисов

$$B_i^* \equiv B_i \bmod \text{М}_{\text{раб}}, \quad (17)$$

где B_i, B_i^* – ортогональные базисы полной и безызбыточной системы оснований.

Тогда ортогональный базис B_i представляется как

$$B_i = \left\lfloor B_i (\text{М}_{\text{раб}})^{-1} \right\rfloor \text{М}_{\text{раб}} + B_i^* = K_i \text{М}_{\text{раб}} + B_i^*. \quad (18)$$

Известно, что значения интервала числа L крутятся по модулю $\text{М}_{\text{конт}} = m_{k+1} m_{k+2}$. Значит, выражение (15) можно заменить следующим равенством

$$L = \left\lfloor \left(\sum_{i=1}^{k+2} x_i (K_i \text{М}_{\text{раб}} + B_i^*) - R\text{М}_{\text{полн}} \right) \Big/ \text{М}_{\text{раб}} \right\rfloor = \left| \sum_{i=1}^{k+2} x_i K_i + R^* \right| \bmod \text{М}_{\text{конт}}, \quad (19)$$

где $R^* = \left\lfloor \sum_{j=1}^{k} x_j B_j^* \Big/ \text{М}_{\text{раб}} \right\rfloor$ – ранг системы безызбыточного МК.

Если комбинация не имеет ошибки, то $X = (x_1, x_2, ..., x_k) < \text{М}_{\text{раб}}$ и значение $L = 0$. В противном случае, при наличии ошибки, $X = (x_1, x_2, ..., x_k) > \text{М}_{\text{раб}}$ и $L > 0$. По величине интервального номера можно определить местоположение и глубину ошибки.

Результаты исследования и их обсуждение

Пусть заданы основания МК $p_1 = 11$, $p_2 = 13$, $p_3 = 19$, которые обладают $g = 2$. Диапазон МК будет составлять $\text{М}_{\text{раб}} = 2717$. Выбираем значение секретных параметров и представляем их в СОК: $U = 15 = (4, 2, 15)$, $S = 7 = (7, 7, 7)$, $T = 5 = (5, 5, 5)$. Вычислим истинный статус спутника:

$$C_1 = g^{U_1} g^{S_1} g^{T_1} \bmod m_1 = \left|2^4 \cdot 2^7 \cdot 2^5\right|_{11}^{+} = \left|2^6\right|_{11}^{+} = 9;$$

$$C_2 = g^{U_2} g^{S_2} g^{T_2} \bmod m_2 = \left|2^2 \cdot 2^7 \cdot 2^5\right|_{13}^{+} = \left|2^2\right|_{13}^{+} = 4;$$

$$C_3 = g^{U_3} g^{S_3} g^{T_3} \bmod m_3 = \left|2^{15} \cdot 2^7 \cdot 2^5\right|_{19}^{+} = \left|2^9\right|_{19}^{+} = 18.$$

Значение $C = (9, 4, 18)$ записывается в память КА.

Пусть «зашумление» равно $\Delta U = 3$, $\Delta S = 5$, $\Delta T = 9$. Тогда получаем зашумленные значения $U^* = (7, 5, 18)$, $S^* = (1, 12, 12)$ и $T^* = (3, 1, 14)$. Вычислим зашумленный статус спутника

$$C_1^* = g^{\mathrm{K}_1^*} g^{S_1^*} g^{T_1^*} \bmod p_1 = \left(2^7 \cdot 2^1 \cdot 2^3\right) \bmod 11 = 2^{11} \bmod 11 = 2,$$

$$C_2^* = g^{\mathrm{K}_2^*} g^{S_2^*} g^{T_2^*} \bmod p_2 = \left(2^5 \cdot 2^{12} \cdot 2^1\right) \bmod 13 = 2^6 \bmod 13 = 12,$$

$$C_3^* = g^{\mathrm{K}_3^*} g^{S_3^*} g^{T_3^*} \bmod p_3 = \left(2^{18} \cdot 2^{12} \cdot 2^{14}\right) \bmod 19 = 2^8 \bmod 19 = 9.$$

Зашумленный статус спутника равен $C^* = (2, 12, 9)$. Он записывается в память КА.

Запросчик, увидев спутник, пересылает ему «вопрос» $d = 7 = (7, 7, 7)$. Ответчик вычисляет ответы на поставленный вопрос. Первый ответ в коде СОК равен

$$r_1(1) = \left(U_1^* - dU_1\right) \bmod \varphi(11) = (7 - 7 \cdot 4) \bmod 10 = 9;$$

$$r_2(1) = \left(U_2^* - dU_2\right) \bmod \varphi(13) = (5 - 7 \cdot 2) \bmod 12 = 3;$$

$$r_3(1) = \left(U_3^* - dU_3\right) \bmod \varphi(19) = (18 - 7 \cdot 15) \bmod 18 = 3.$$

Второй ответ на поставленный вопрос, представленный в коде СОК, имеет вид

$$r_1(2) = \left(S_1^* - dS_1\right) \bmod \varphi(11) = (1 - 7 \cdot 7) \bmod 10 = 2;$$

$$r_2(2) = \left(S_2^* - dS_2\right) \bmod \varphi(13) = (12 - 7 \cdot 7) \bmod 12 = 11;$$

$$r_3(2) = \left(S_3^* - dS_3\right) \bmod \varphi(19) = (12 - 7 \cdot 7) \bmod 18 = 17.$$

Третий ответ на поставленный вопрос, представленный в коде СОК, имеет вид

$$r_1(3) = \left(T_1^* - dT_1\right) \bmod \varphi(11) = (3 - 7 \cdot 5) \bmod 10 = 8;$$

$$r_2(3) = \left(T_2^* - dT_2\right) \bmod \varphi(13) = (1 - 7 \cdot 5) \bmod 12 = 2;$$

$$r_3(3) = \left(T_3^* - dT_3\right) \bmod \varphi(19) = (14 - 7 \cdot 5) \bmod 18 = 15.$$

Вычисленные истинный и зашумленный статусы, а также ответы передаются ответчику. Ответчик проверяет статус спутника. Для этого вычисляется

$$A_1 = C_1^d g^{r(1)_1} g^{r(2)_1} g^{r(3)_1} \bmod p_1 = \left(9^7 \cdot 2^9 \cdot 2^2 \cdot 2^8\right) \bmod 11 = 2^1 \bmod 11 = 2;$$

$$A_2 = C_2^d g^{r(1)_2} g^{r(2)_2} g^{r(3)_2} \bmod p_2 = \left(4^7 \cdot 2^3 \cdot 2^{11} \cdot 2^2\right) \bmod 13 = 2^6 \bmod 13 = 12;$$

$$A_3 = C_3^d g^{r(1)_3} g^{r(2)_3} g^{r(3)_3} \bmod p_3 = \left(18^7 \cdot 2^3 \cdot 2^{17} \cdot 2^{15}\right) \bmod 19 = 2^8 \bmod 19 = 9.$$

Так как $A_1 = C_1^* \bmod p_1 = 2$, $A_2 = C_2^* \bmod p_2 = 12$, $A_3 = C_3^* \bmod p_3 = 9$, то спутник аутентифицируется как «свой», и начинается обмен данными между КА и объектом.

Рассмотрим выполнение разработанного поиска и коррекции ошибок. Пусть заданы рабочие основания $p_1 = 11$, $p_2 = 13$, $p_3 = 19$. Тогда рабочий диапазон модулярного кода составит $\mathrm{M}_{\text{раб}} = 2717$. В качестве контрольных оснований выбираем $p_4 = 29$, $p_2 = 37$. Это приводит к расширению диапазона $M = 2915341$. При этом $\mathrm{M}_{\text{конт}} = 1073$. Ортогональные базисы равны

$$B_1 = \mathrm{K}_1 \mathrm{M}_{\text{раб}} + B_1^* = 682 \cdot \mathrm{M}_{\text{раб}} + 2223 = 1855217;$$

$$B_2 = \mathrm{K}_2 \mathrm{M}_{\text{раб}} + B_2^* = 165 \cdot \mathrm{M}_{\text{раб}} + 209 = 448514;$$

$$B_3 = \text{К}_3\text{М}_{\text{раб}} + B_3^* = 847 \cdot \text{М}_{\text{раб}} + 286 = 2301585;$$

$$B_4 = \text{К}_4\text{М}_{\text{раб}} = 74 \cdot \text{М}_{\text{раб}} = 201058;$$

$$B_5 = \text{К}_5\text{М}_{\text{раб}} = 377 \cdot \text{М}_{\text{раб}} = 1024309.$$

Пусть на вход устройства поступает разрешенная комбинация $A = 401 = (5, 11, 2, 24, 31)$. Вычислим значение ранга безызбыточного МК по основаниям $p_1 = 11$, $p_2 = 13$, $p_3 = 19$.

$$R^* = \left[\sum_{i=1}^{3} \alpha_i B_i^* \Big/ \text{М}_{\text{раб}}\right] = \left[5 \cdot 2223 + 11 \cdot 209 + 2 \cdot 286/2717\right] = 5.$$

Воспользуемся алгоритмом (19) для вычисления интервального номера числа

$$l = \left|\sum_{i=1}^{5} \alpha_i K_i + R\right|_{P_{\text{конт}}}^{+} = \left|5 \cdot 682 + 11 \cdot 165 + 2 \cdot 847 + 24 \cdot 74 + 31 \cdot 377 + 5\right|_{1073}^{+} = 0.$$

Так как интервальный номер равен нулю, то это означает, что кодовая комбинация числа $A = 401 = (5, 11, 2, 24, 31)$ является разрешенной и не содержит ошибки.

Пусть в процессе вычислений произошла ошибка, которая исказила первый остаток. Тогда комбинация имеет вид $A^* = (7, 11, 2, 24, 31)$. Тогда значение ранга безызбыточного модулярного кода по основаниям

$$R^* = \left[\sum_{i=1}^{3} \alpha_i B_i^* \Big/ \text{М}_{\text{раб}}\right] = \left[7 \cdot 2223 + 11 \cdot 209 + 2 \cdot 286/2717\right] = 6.$$

Вычислим значение интервального номера $A^* = (7,11,2, 24, 31)$, используя (19). Получаем

$$l = \left|\sum_{i=1}^{5} \alpha_i K_i + R\right|_{P_{\text{конт}}}^{+} = \left|7 \cdot 682 + 11 \cdot 165 + 2 \cdot 847 + 24 \cdot 74 + 31 \cdot 377 + 6\right|_{1073}^{+} = 292.$$

Так как $L = 292$, то комбинация числа $A^* = (7, 11, 2, 24, 31)$ содержит ошибку. Данное значение интервала соответствует вектору ошибки $\Delta_{\text{корр}} = (9, 0, 0)$. Исправим ошибку

$$A^* + \Delta_{\text{корр}} = (7,11,2) + (9,0,0) = \left(\left|7+9\right|_{11}^{+}, \left|11+0\right|_{13}^{+}, \left|2+0\right|_{19}^{+}\right) = (5,11,2).$$

Заключение

В статье представлены новые принципы построения запросно-ответной системы распознавания спутника в модулярном коде. Так как скорость выполнения мультипликативных операций пропорциональна разрядности операндов, то применение 5-разрядных оснований в рассмотренном примере позволило повысить скорость вычислений более чем в 2 раза, по сравнению с использованием 12-разрядного модуля q. Кроме того применение МК повышает отказоустойчивость запросно-ответной системы распознавания спутника. Разработанный алгоритм вычисления ПХ интервальный номер позволяет исправлять 100 % однократных ошибок, которые возникают в процессе работы ЗОСРС. Данное направление является перспективой применения модулярных кодов для построения отказоустойчивых запросно-ответных систем распознавания спутника.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 17-37-50017.

Список литературы

1. Калмыков М.И., Саркисов А.Б., Петрова Е.В. Способ построения системы опознавания «свой-чужой» на основе протокола протокола с нулевым разглашением. Патент 2570700. 2015. Бюл. № 34.

2. Червяков Н.И., Коляда А.А., Ляхов П.А. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях / Н.И. Червяков, А.А. Коляда, П.А. Ляхов. – М.: ФИЗМАТЛИТ, 2017. – 400 с.

3. Ananda Mohan Residue Number Systems. Theory and Applications // Springer International Publishing Switzerland. – 2016 – 351 p.

4. Пашинцев В.П., Калмыков М.И., Ляхов А.В. Применение помехоустойчивого протокола аутентификации космического аппарата для низкоорбитальной системы спутниковой связи // Инфокоммуникационные технологии. – 2015. – № 2. – С. 183–190.

5. Omondi A. and Premkumar B. Residue Number Systems: Theory and Implementation. Imperial College Press. UK 2007. – 296 p.

6. Yones D. Comparative Study on Different Moduli Sets in RNS. International Conference on Computer System and Industrial Informatics (ICCSII). – 2012. – P. 1–6.

7. Резеньков Д.Н., Горденко Д.В., Саркисов А.Б. Методы и алгоритмы реконфигурации непозиционных вычислительных структур для обеспечения отказоустойчивости спецпроцессоров. – Ставрополь: Издательско-информационный центр «Фабула», 2014. – 180 с.

8. Mohan P.V. Residue Number Systems. Algorithms and Architectures. Springer Science + Business Media New York. – 2002. – 254 p.

9. Kalmykov I.A., Katkov K.A., Timoshenko L.I., Dunin A.V., Gish, T.A. Application of Modular Technologies in the Large-Scale Analysis of Signals // Journal of Theoretical and Applied Information Technology. – 2015. – № 80(3). – P. 391–400.