УДК 004.052.2:629.78

РЕАЛИЗАЦИЯ АЛГОРИТМОВ ВЫПОЛНЕНИЯ ПРЯМОГО ПРЕОБРАЗОВАНИЯ ИЗ ПОЗИЦИОННОГО КОДА В МОДУЛЯРНЫЙ КОД ДЛЯ СИСТЕМЫ АУТЕНТИФИКАЦИИ КОСМИЧЕСКОГО АППАРАТА

[1]Калмыков М.И., [1]Степанова Е.П., [1]Ефременков И.Д., [1]Ефимович А.В., [1]Калмыков И.А., [2]Тынчеров К.Т.

[1]ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru;
[2]Филиал ФГАОУ ВО «Уфимский государственный нефтяной технический университет», Октябрьский

Для эффективного функционирования автоматизированных систем дистанционного контроля и управления экологически опасными объектами, которые располагаются в районах Крайнего Севера, необходимо использовать низкоорбитальные системы спутниковой связи (НССС). Так как орбита НССС не превышает 1500 км, то для обеспечения бесперебойной связи в состав группировки включают до 60 спутников. Так как количество стран и компаний, осваивающих недра Северного Ледовитого океана, постоянно возрастает, то увеличивается и число группировок НССС. Для повышения информационной скрытности НССС и предотвращения навязывания имитированной команды управления целесообразно применять систему аутентификации космического аппарата. Такая система, определив статус аппарата, не предоставит сеанс связи спутнику-нарушителю. Очевидно, что информационная скрытность низкоорбитальной системы спутниковой связи будет определяться протоколом аутентификации. Для сокращения временных затрат на аутентификации спутника используются модулярные коды, в которых вычисления осуществляются параллельно и независимо от друг от друга. Так как данные коды являются непозиционными и работают с вычетами, то первой обязательной операцией является преобразование из позиционного кода в модулярный код. Целью исследований является снижение временных затрат на выполнение прямого преобразования для систем аутентификации космического аппарата, функционирующей в модулярных кодах.

Ключевые слова: система аутентификации космического аппарата, протокол аутентификации, модулярные коды, алгоритмы преобразования из позиционного кода в модулярный код

IMPLEMENTATION OF ALGORITHMS FOR PERFORMING DIRECT CONVERSION OF THE POSITIONAL CODE INTO MODULAR CODE FOR THE AUTHENTICATION SYSTEM OF THE SPACECRAFT

[1]Kalmykov M.I., [1]Stepanova E.P., [1]Efremenkov I.D., [1]Efimovich A.V., [1]Kalmykov I.A., [2]Tyncherov K.T.

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

For the effective functioning of automated systems for remote control and management of environmentally hazardous objects, which are located in the Far North, it is necessary to use low-orbit satellite communication systems (LOSCS). Since the orbit of the LOSCS does not exceed 1500 km, up to 60 satellites are included in the constellation to ensure uninterrupted communication. Since the number of countries and companies developing the bowels of the Arctic ocean is constantly increasing, the number of NSSs groups is also increasing. In order to increase the information secrecy of the LOSCS s and prevent the imposition of a simulated command control, it is advisable to use a system of authentication of the spacecraft. Such a system, having determined the status of the device, will not provide a communication session to the satellite-intruder. It is obvious that the information secrecy of the low-orbit satellite communication system will be determined by the authentication Protocol. To reduce the time spent on satellite authentication, modular codes are used, in which calculations are performed in parallel and independently of each other. Since these codes are non-positional and work with deductions, the first mandatory operation is the conversion from the positional code to the modular code. The aim of the research is to reduce the time required to perform a direct conversion for spacecraft authentication systems operating in modular codes.

Keywords: spacecraft authentication system, authentication protocol, modular codes, conversion algorithms from position code to modular code

Так как многие объекты управления размещаются в труднодоступных местах за полярным кругом, то организация с центром управления осуществляется с использованием низкоорбитальных систем спутниковой связи (НССС). Так как число группировок НССС постоянно будет возрастать, то может получиться ситуация, когда в зоне видимости приемной станции спутниковой связи, находящейся на необслуживаемом объекте управления, появится спутник-нарушитель. С целью противодействия навязыванию ранее перехваченной команды управления, в работе [1] предлагается использовать систему аутентификации космического аппарата (КА). Очевидно, что уровень информационной скрытности НССС будет определяться протоколом ау-

тентификации, которые в своем алгоритме используют большие простые числа. Для снижения временных затрат, необходимых на проверку статуса космического аппарата, в работе [2] предлагается использовать модулярные коды (МК). Но прежде чем производить вычисления в МК, необходимо осуществить прямое преобразование из позиционной системы счисления (ПСС) в МК. Поэтому разработка алгоритмов прямого преобразования ПСС-МК, требующих минимальных временных затрат, является актуальной задачей.

Цель исследования: с целью повышения информационной скрытности НССС в системе определения статуса КА используют протоколы аутентификации, которые базируются на доказательстве с нулевым разглашением знаний. Для обеспечения высокой криптостойкости в таких протоколах используются большие простые числа, что приводит к увеличению временных и схемных затрат. Использование МК в протоколах аутентификации КА позволяет повысить скорость вычислений, так как операции сложения, вычитания и умножения выполняются параллельно и с малоразрядными операндами по основаниям p_1, p_2, ..., p_k. Однако для перехода от позиционного кода к модулярному коду необходимо выполнить обязательную операцию – прямое преобразование ПСС-МК, что приводит к увеличению временных затрат. Целью исследований является снижение временных затрат на выполнение прямого преобразования ПСС-МК для систем аутентификации КА, функционирующей в МК.

Материалы и методы исследования

Интеграция свойств модулярных кодов в протоколы аутентификации, использующие доказательство с нулевым разглашением знаний, позволила повысить скорость выполнения определения статуса спутника. Основу МК составляют остатки, которые получаются путем делении целого числа X на основания системы $p_1, p_2, ..., p_k$. Тогда модулярный код имеет вид

$$X = (x_1, x_2, ..., x_k), \tag{1}$$

где $x_i \equiv X \bmod p_i$; $i = 1,...,k$; НОД(p_i, p_j) = 1; $i \neq j$.

Как показано в работах [3–5], непозиционный МК позволяет повысить скорость выполнения модульных операций сложения, вычитания и умножения, так как справедливо

$$\left|X + Y\right|_{p_i}^{+} = (\left|x_1 + y_1\right|_{p_1}^{+}, \left|x_2 + y_2\right|_{p_2}^{+}, ..., \left|x_k + y_k\right|_{p_k}^{+}), \tag{2}$$

$$\left|X - Y\right|_{p_i}^{+} = (\left|x_1 - y_1\right|_{p_1}^{+}, \left|x_2 - y_2\right|_{p_2}^{+}, ..., \left|x_k - y_k\right|_{p_k}^{+}), \tag{3}$$

$$\left|X \cdot Y\right|_{p_i}^{+} = (\left|x_1 \cdot y_1\right|_{p_1}^{+}, \left|x_2 \cdot y_2\right|_{p_2}^{+}, ..., \left|x_k \cdot y_k\right|_{p_k}^{+}), \tag{4}$$

где $x_i \equiv X \bmod p_i$; $y_i \equiv Y \bmod p_i$; $X = \left(x_1, x_2, ..., x_k\right)$ и $Y = \left(y_1, y_2, ..., y_k\right)$ – модулярный код.

При этом набор оснований в МК выбирают так, чтобы операнды X, Y, а также результаты вычислений не выходили за пределы рабочего диапазона, определяемого как

$$P_{\text{раб}} = \prod_{i=1}^{k} p_i. \tag{5}$$

Рассмотрим протокол аутентификации КА, реализованный МК, который использует секретный ключ $U = (u_1, ,..., u_k)$, сеансовый ключ $S(j) = (S_1(j), ..., S_k(j))$, параметр $T(j) = (T_1(j), ..., T_k(j))$, применяемый для проверки повторного использования сеансового ключа, где $U \equiv u_i \bmod p_i$; $S(j) \equiv S_i(j) \bmod p_i$; $T(j) \equiv T_i(j) \bmod p_i$; $i = 1, 2,\ldots, k$. Протокол состоит в следующем.

1. На борту КА происходит вычисление истинного статуса КА, представленного в МК

$$C_i = \left| g^{u_i} g^{S_i(j)} g^{T_i(j)} \right|_{p_i}^{+}, \tag{6}$$

где g – порождающий мультипликативную группу по модулю p_i; $i = 1, 2,\ldots, k$.

2. Затем на борту КА производится «зашумление» параметров протокола

$$u_i^* = \left| u_i + \Delta u_i \right|_{p_i}^{+}; \; S_i^*(j) = \left| S_i(j) + \Delta S_i(j) \right|_{p_i}^{+}; \; T_i^*(j) = \left| T_i(j) + \Delta T_i(j) \right|_{p_i}^{+}. \tag{7}$$

где $\Delta U, \Delta S(j), \Delta T(j)$ – случайные значения; $\Delta U \equiv \Delta u_i \bmod p_i$; $\Delta S(j) \equiv \Delta S_i(j) \bmod p_i$; $\Delta T(j) \equiv \Delta T_i(j) \bmod p_i$; $i = 1, 2,\ldots, k$.

3. На борту КА определяется зашумленный статус космического аппарата в МК

$$C_i^* = \left| g^{u_i^*} g^{S_i^*(j)} g^{T_i^*(j)} \right|_{m_i}^{+}. \tag{8}$$

4. При аутентификации КА запросчик передает случайное число $d = (d_1,\ldots, d_k)$.
5. Спутник, получив «вопрос» $d = (d_1,\ldots, d_k)$, вычисляет ответы на него

$$r_i\ (1) = \left|u_i^* - d_i\, u_i\right|_{\varphi(p_i)}^{+};\ r_i\ (2) = \left|S_i^*(j) - d_i\, S_i\ (j)\right|_{\varphi(p_i)}^{+};\ r_i\ (3) = \left|T_i^*(j) - d_i\, T_i\ (j)\right|_{\varphi(p_i)}^{+}. \quad (9)$$

6. Спутник, передает запросчику истинный и зашумленный статусы, а также ответы на поставленный «вопрос» d.
7. Запросчик производит аутентификацию КА согласно

$$Y_i = \left|C_i^{d_i}\, g^{r_i\ (1)} g^{r_i\ (2)} g^{r_i\ (3)}\right|_{p_i}^{+}. \quad (10)$$

Если полученный результат совпадает с зашумленным статусом, то запросчик считает спутник «своим».

Очевидно, что для осуществлений вычислений в МК необходимо выполнить прямое преобразование из ПСС в модулярный код. Известно, что данная операция считается немодульной и ее временные затраты определяются соответствующими алгоритмом [3–5]. Получить остаток числа X по модулю p_i, где $i = 1, 2,\ldots, k$, можно путем простого деления, т.е.

$$x_i = X - \left[X/p_i\right] p_i, \quad (11)$$

где $\left[X/p_i\right]$ – наименьшее целое от деления целого числа X на основание p_i.

Так как модулярный код, который задан взаимно простыми основаниями $p_1, p_2,..., p_k$, представляет собой алгебраическую систему кольца, то в данной системе отсутствует операция деления. Это привело к необходимости разработки алгоритмов вычисления остатка через последовательность модульных операций.

Так, в работе [5] представлен алгоритм вычисления остатка на основании метода уменьшения разрядности. Данный алгоритм базируется на свойствах сравнимости. Представим исходное число X в двоичном коде, где разряды $0 \le X_j \le 1$. Тогда имеем

$$X = X_n 2^n + X_{n-1} 2^{n-1} + X_{n-2} 2^{n-2} + \ldots + X_1\, 2^1 + X_0\, 2^0 = \sum_{j=0}^{n} X_j\, 2^j. \quad (12)$$

Затем вычисляются остатки по модулю p_i каждого веса двоичного кода числа X

$$C_j \equiv X_j \bmod p_i = 2^j \bmod p_i. \quad (13)$$

Полученные значения C_j подставляются вместо степеней двойки в выражение (12). Используя свойство сравнимости, получаем сумму

$$X = X_n C_n + X_{n-1} C_{n-1} + \ldots + X_1\, C_1 + X_0 C_0 \equiv Z_1 \bmod p_i. \quad (14)$$

Очевидно, что полученное значение Z_1 будет иметь меньшую разрядность, чем исходное число X. Затем алгоритм выполняется с числом Z_1. В результате будет получено число Z_2 меньшей размерности, чем Z_1. Алгоритм будет повторяться до тех пор, пока не будет получена сумма, удовлетворяющая условию $Z_L < p_i$. Полученный результат и будет остатком числа X по модулю p_i

$$x_i = Z_L \equiv X \bmod p_i. \quad (15)$$

Основным достоинством данного алгоритма, использующего понижение разрядности, является использование при определении остатка простого позиционного сумматора. Несмотря на простоту схемной реализации, данный алгоритм имеет недостатки:

– значительные временные затраты при большой разрядности операнда X;
– необходимо осуществлять проверку окончания процесса после каждой итерации.

Наряду с алгоритмами с понижением разрядности в вычислительных устройствах, функционирующих в модулярном коде, применяются алгоритмы, использующие методы непосредственного суммирования [3, 4]. В основу данных алгоритмов положено использование констант, которые представляют собой остатки по модулю p_i всех степеней оснований 2^j и коэффициентов при соответствующих степенях оснований X_j, то есть

$$x_i = X \bmod p_i = \left|\sum_{j=0}^{n} X_j \left|2^j\right|_{p_i}^{+}\right|_{p_i}^{+}. \quad (16)$$

Тогда последовательный алгоритм преобразования ПСС-МК имеет вид

$$\left|X\right|_{p_i}^{+} = \left|\left|2^{n-1} a_{n-1}\right|_{p_i}^{+} + \left|2^{n-2} a_{n-2}\right|_{p_i}^{+} + \left|2^{n-3} a_{n-3}\right|_{p_i}^{+} + \ldots + \left|2^1 a_1\right|_{p_i}^{+} + \left|2^0 a_0\right|_{p_i}^{+}\right|_{p_i}^{+}. \quad (17)$$

Структурная модель, реализующая алгоритм (17), показана на рис. 1.

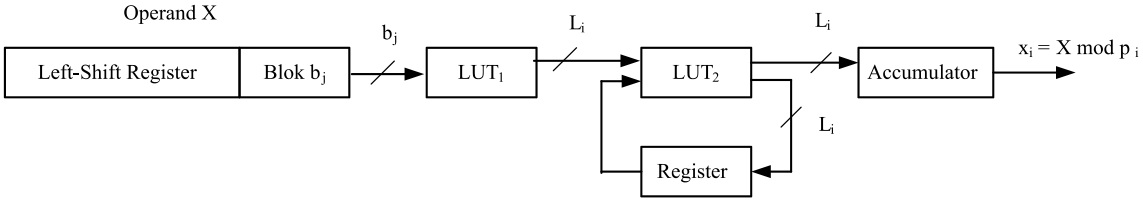

Рис. 1. Структурная модель выполнения последовательного алгоритма ПСС-МК

Операнд X, представленный в ПСС, записывается в регистр сдвига на b_j разрядов, где $b_j = 1,...,L_i = \lceil \log p_i \rceil$. Блок из b_j разрядов поступает на первую просмотровую таблицу (LUT_1), с выхода которой снимается значение остатка по модулю p_i степеней оснований 2^j при соответствующих значениях коэффициентов X^j. Вторая просмотровая таблица (LUT_2) выполняет последовательное вычисление остатка по модулю p_i. Промежуточный результат записывается в регистр (Register). По окончанию алгоритма вычисленное значение остатка числа X по модулю p_i подается в аккумулятор (Accumulator), а затем на выход. При реализации алгоритма (17) время вычисления остатка числа по модулю составит

$$T^1_{\text{ПСС– СОК}} = t_{LUT}\, n/b_j + t_{ACC}, \tag{18}$$

где t_{LUT} – время выборки из LUT-таблицы; t_{ACC} – время срабатывания аккумулятора.

Основным достоинством последовательного алгоритма вычисления остатка числа X по модулю являются низкие схемные затраты на реализацию прямого преобразования ПСС-МК. Однако данный алгоритм имеет недостаток – значительные временные затраты, которые увеличиваются при увеличении разрядности операнда X.

С целью устранения данного недостатка был модифицирован алгоритм параллельного определения остатка на основе распределенной арифметики. Для этого двоичный код числа разбивается на блоки, состоящие из B разрядов

$$\begin{aligned} |X|^+_{p_i} &= (\left|2^n a_n + ... + 2^{n-B} a_{n-B}\right|^+_{p_i} + \left|2^{n-B-1} a_{n-B-1} + ... + 2^{n-2B} a_{n-2B}\right|^+_{p_i} + \\ &+ ... + \left|2^{B-1} a_{B-1} + ... + 1\right|^+_{p_i}) \bmod p_i = (B_L + B_{L-1} + ... + B_1) \bmod p_i . \end{aligned} \tag{19}$$

Затем определяются остатки по модулю каждого из блоков $B_1,\ldots, B_L$ согласно

$$\begin{aligned} \left|B_1\right|^+_p &= \left|2^{B-1} a_{B-1} + ... + 2^0 a_0\right|^+_p = \left|\left|2^0\right|^+_p (a^1_{B-1} + ... + a^1_0)\right|^+_p , \\ &\vdots \\ \left|B_L\right|^+_p &= \left|2^n a_n + ... + 2^{n-B} a_{n-B}\right|^+_p = \left|\left|2^{n-B}\right|^+_p (a^L_{B-1} + ... + a^L_0)\right|^+_p , \end{aligned} \tag{20}$$

где $2^{(j+1)B-1} a_{B-1} + ... + 2^{jB} a_B = 2^{jB}(a^j_{B-1} + ... + a^j_0)$; $(a^j_{B-1} + ... + a^j_0)$ – двоичный код B_j блока.

На рис. 2 представлена структурная модель, реализующая модифицированный алгоритм параллельного определения остатка на основе распределенной арифметики (20). Временные затраты при использовании модификации алгоритма (20) составят

$$T_{FC} = t_{LUT} + t_{LUT} \times \log_2 \lceil n/B \rceil, \tag{21}$$

где B – размер блока; n – размер входного операнда; t_{LUT} – время выборки из LUT-таблицы.

Результаты исследования и их обсуждение

Пусть необходимо вычислить остаток числа $X = 32015$ по модулю $p = 17$. Представим в двоичном коде число $X = 32015 = 0111\ 1101\ 0000\ 1111_2$. Воспользуемся последовательным алгоритмом (12) при длине блока $b_j = 1$. Тогда получаем

$$\begin{aligned} |32015|^+_{17} &= |1111101000111|^+_{17} = \left|2^{14} + 2^{13} + 2^{12} + 2^{11} + 2^{10} + 2^8 + 2^3 + 2^2 + 2^1 + 1\right|^+_{17} = \\ &\left|\left|2^{14}\right|^+_{17} + \left|2^{13}\right|^+_{17} + \left|2^{12}\right|^+_{17} + \left|2^{11}\right|^+_{17} + \left|2^{10}\right|^+_{17} + \left|2^8\right|^+_{17} + \left|2^3\right|^+_{17} + \left|2^2\right|^+_{17} + \left|2^1\right|^+_{17} + \left|2^0\right|^+_{17}\right|^+_{17} = 4. \end{aligned}$$

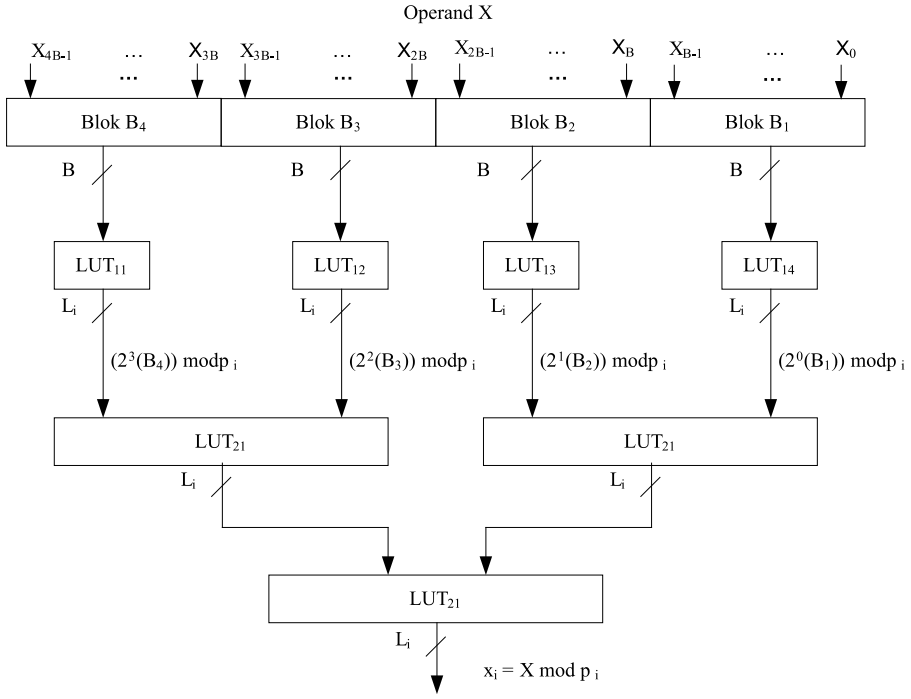

Рис. 2. Структурная модель, реализующая алгоритм (20) ПСС-МК

Согласно (18) время вычисления остатка при условии $t_{LUT} = t_{ACC}$ составит

$$T^1_{\text{ПСС–СОК}} = 2t_{LUT}\, n/b_j + t_{ACC} = 16t_{LUT}/1 + t_{LUT} = 17t_{LUT}.$$

Сократим время вычисления остатка, увеличив размерности блока $b_j = 2$. В этом случае число $X = 32015_{10} = 01\ 11\ 11\ 01\ 00\ 00\ 11\ 11_2$. Тогда

$$|32015|^+_{17} = \left|\left|1\cdot 2^{14}\right|^+_{17} + \left|3\cdot 2^{12}\right|^+_{17} + \left|3\cdot 2^{10}\right|^+_{17} + \left|1\cdot 2^{8}\right|^+_{17} + \left|3\cdot 2^{2}\right|^+_{17} + \left|3\cdot 2^{0}\right|^+_{17}\right|^+_{17} =$$

$$= \left|\left|1\cdot 13\right|^+_{17} + \left|3\cdot 16\right|^+_{17} + \left|3\cdot 4\right|^+_{17} + \left|1\cdot 1\right|^+_{17} + \left|3\cdot 4\right|^+_{17} + \left|3\cdot 1\right|^+_{17}\right|^{+\ +}_{1717} = 4.$$

В этом случае время вычисления остатка составит

$$T^1_{\text{ПСС–СОК}} = t_{LUT}\, n/b_j + t_{ACC} = 16t_{LUT}/2 + t_{LUT} = 9t_{LUT}.$$

Рассмотрим модифицированный алгоритм параллельного определения остатка на основе распределенной арифметики (15). Двоичный код числа $X = 32015$ разобьем на блоки по $B = 4$ бит. Тогда получаем $X = 32015 = 0111\ 1101\ 0000\ 1111$. В результате получили 4 числа $B_4 = 7$, $B_3 = 13$, $B_2 = 0$, $B_1 = 15$. Тогда остаток по модулю 17 будет равен

$$|32015|^+_{17} = \left|\left|7\cdot 2^{12}\right|^+_{17} + \left|13\cdot 2^{8}\right|^+_{17} + \left|0\cdot 2^{4}\right|^+_{17} + \left|15\cdot 2^{0}\right|^+_{17}\right|^+_{17} =$$

$$= \left|\left|7\cdot 16\right|^+_{17} + \left|13\cdot 1\right|^+_{17} + \left|0\cdot 16\right|^+_{17} + \left|15\cdot 1\right|^+_{17}\right|^+_{17} = \left|10+13+0+15\right|^+_{17} = 4.$$

Временные затраты при использовании модификации алгоритма (20) составят

$$T_{FC} = t_{LUT} + t_{LUT} \times \log_2 \lceil n/B \rceil = 3t_{LUT}.$$

Проведенные исследования показали, что использование модификации алгоритма параллельного определения остатка на основе распределенной арифметики позволяет обеспечить максимальную скорость вычисления остатка числа. Применение данного алгоритма при обработке 16-разрядных операндов позволило сократить временные затраты в 5,67 раз по сравнению с последовательным алгоритмом (17) при $b_j = 1$ и в 3 раза – при использовании длины блока, равной $b_j = 2$.

Заключение

Для снижения временных затрат, необходимых на проверку статуса космического аппарата, используются модулярные коды. Но прежде чем будет выполняться протокол аутентификации в МК, необходимо осуществить прямое преобразование из позиционной системы счисления в МК. Поэтому разработка алгоритмов прямого преобразования ПСС-МК, требующих минимальных временных затрат, является актуальной задачей. В статье представлена модификация алгоритма параллельного определения остатка на основе распределенной арифметики. Проведенные исследования показали, что применение данного алгоритма при обработке 16-разрядных операндов позволило сократить временные затраты в 5,67 раз по сравнению с последовательным алгоритмом при $b_j = 1$ и в 3 раза – при использовании длины блока равной $b_j = 2$. Полученные результаты свидетельствуют о целесообразности разработанного алгоритма прямого преобразования в системах аутентификации космического аппарата, функционирующего в модулярных кодах.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-07-01020.

Список литературы

1. Калмыков И.А., Вельц О.В., Калмыков М.И. Алгоритм имитозащиты для системы удаленного мониторинга и управления критическими технологиями // Известия ЮФУ. Технические науки. 2014. № 2 (151). С. 181–187.

2. Pashintsev, V.P., Zhuk, A.P., Rezenkov, D.N. Application of spoof resistant authentication protocol of spacecraft in low earth orbit systems of satellite communication. International Journal of Mechanical Engineering and Technology. 2018. № 9 (5). P. 958–965.

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

4. Ananda Mohan Residue Number Systems. Theory and Applications. Springer International Publishing Switzerland, 2016. 734 p.

5. Omondi A., Premkumar B. Residue Number Systems: Theory and Implementation. Imperial College Press. UK, 2007. 657 p.