УДК 004.052.2

РАЗРАБОТКА АЛГОРИТМА КОРРЕКЦИИ ОШИБОК ДЛЯ ПОВЫШЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ СИСТЕМЫ ОПОЗНАВАНИЯ «СВОЙ-ЧУЖОЙ»

Калмыков И.А., Степанова Е.П., Калмыкова Н.И., Павлюк Д.Н.
ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru

В качестве одного из способов, позволяющих увеличить информационную скрытность низкоорбитальной системы спутниковой связи, можно выделить систему опознавания «свой-чужой». Применение такой системы позволяет перед началом сеанса «спутник-Земля» провести аутентификацию космического аппарата. Если статус спутника окажется «свой», то система опознавания предоставляет сеанс связи. С целью сокращения времени на аутентификацию в ряде работ предлагается перейти к применению полиномиального модулярного кода (ПМК). Данный код представляет собой набор остатков, которые получены при делении исходного числа на выбранные неприводимые многочлены, которые являются основаниями ПМК. В результате этого операции сложения, вычитания и умножения можно заменить соответствующими операциями над остатками. В результате того что остатки имеют маленькую разрядность, а отмеченные выше операции выполняются параллельно, использование полиномиальных модулярных кодов позволяет повысить скорость проводимых вычислений. Таким образом, использование параллельности ПМК сокращает время на вычисление ответов на поставленный вопрос запросчика. В результате этого сокращается время, необходимое на опознавание спутника. Однако если в данный код ввести избыточность, то он будет способен осуществлять поиск и коррекцию ошибки. В результате применения избыточного ПМК повышается отказоустойчивость системы опознавания. Цель работы – разработать алгоритм коррекции ошибок в полиномиальных модулярных кодах, применение которого позволит повысить отказоустойчивость системы «свой-чужой».

Ключевые слова: система опознавания, протокол аутентификации спутника, полиномиальные модулярные коды, алгоритм поиска и коррекции ошибок, синдром ошибки

DEVELOPMENT OF AN ERROR CORRECTION ALGORITHM TO IMPROVE THE FAULT TOLERANCE OF THE IDENTIFICATION-FRIEND-OR-FOE

Kalmykov I.A., Stepanova E.P., Kalmykova N.I., Pavlyuk D.N.
Federal State Autonomous Educational Institution Higher Professional Education «North-Caucasian Federal University», Stavropol, e-mail: kia762@yandex.ru

As one of the ways to increase the information secrecy of a low-orbit satellite communication system, we can single out the «friend-foe» identification system. The use of such a system allows you to authenticate the spacecraft before the start of the satellite-Earth session. If the satellite status turns out to be «own», the identification system provides a communication session. In order to reduce the time for authentication, a number of papers suggest switching to the use of polynomial modular code (PMC). This code is a set of residuals that are obtained by dividing the original number by the selected irreducible polynomials that are the bases of the PMK. As a result, the addition, subtraction, and multiplication operations can be replaced with the corresponding operations on the remainder. As a result of the fact that the remainder has a small bit depth, and the operations noted above are performed in parallel, the use of polynomial modular codes allows you to increase the speed of calculations. Thus, the use of parallel PMC reduces the time to calculate the answers to the requester's question. As a result, the time required to identify the satellite is reduced. However, if you enter redundancy in this code, it will be able to search for and correct the error. As a result of the use of excessive PMC, the fault tolerance of the identification system increases. The purpose of this work is to develop an error correction algorithm for polynomial modular codes, which will improve the fault tolerance of the identification-friend-or-foe.

Keywords: identification-friend-or-foe, satellite authentication protocol, polynomial modular codes, error search and correction algorithm, error syndrome

В последнее десятилетие наблюдается тенденция по расширению сферы применения низкоорбитальных систем спутниковой связи (НССС). Невозможно представить себе без НССС развитие Северного морского пути, развертывание подразделений Вооруженных сил Российской Федерации, обеспечивающих безопасность страны в Арктике, а также создание глобальной многофункциональной инфокоммуникационной спутниковой системы [1; 2]. Очевидно, что современные НССС должны обладать высокой информационной скрытностью. В работах [3; 4] для достижения данной цели предлагается использовать систему опознавания «свой-чужой». С целью повышения скорости опознавания спутников НССС в работе [5] предлагается использовать полиномиальные модулярные коды (ПМК), которые обеспечивают параллельную реализацию протокола аутентификации. Однако при введении избыточности полиномиальные модулярные коды могут осуществлять поиск и коррекцию ошибок, что позволит повысить отказоустойчивость системы опознавания «свой-чужой». Поэтому разработка алгоритма коррекции результатов вычислений с помощью ПМК является актуальной задачей.

Для повышения эффективности функционирования системы опознавания спутников предлагается воспользоваться непозиционными полиномиальными модулярными кодами, в которых данные, представленные в виде набора остатков, обрабатываются параллельно. Так как в процессе вычислений обмена между основаниями не происходит, то данное свойство используется для построения кодов, способных осуществлять поиск и коррекцию ошибок. Поэтому целью работы является разработка алгоритма коррекции ошибок в ПМК, применение которого позволит повысить отказоустойчивость системы «свой-чужой».

Материалы и методы исследования

Чтобы получить полиномиальный модулярный код, выбирают кортеж неприводимых полиномов $m_1(x), m_2(x), ..., m_k(x)$ [6; 7]. Их произведение дает рабочий диапазон

$$\hat{M}(x) = \prod_{i=1}^{k} m_i(x). \quad (1)$$

Тогда полином $Y(x)$ можно однозначно описать комбинацией ПМК

$$Y(x) = (y_1(x), y_2(x), ..., y_k(x)), \quad (2)$$

где $y_i(x) \equiv Y(x) \bmod m_i(x)$; $\deg Y(x) < \deg \hat{M}(x)$; $\deg Y(x)$ – степень полинома $Y(x)$.

При этом для арифметических операций, выполняемых в ПМК, справедливо

$$Y(x) \oplus Z(x) = (\left|y_1(x) + z_1(x)\right|_{p_1(x)}, ..., \left|y_k(x) + z_k(x)\right|_{p_k(x)}), \quad (3)$$

$$Y(x) \cdot Z(x) = (\left|y_1(x) \cdot z_1(x)\right|_{p_1(x)}, ..., \left|y_k(x) \cdot z_k(x)\right|_{p_k(x)}), \quad (4)$$

где $Z(x) \equiv z_i(x) \bmod p_i(x)$; $i = 1, 2, ..., k$; $\deg Z(x) < \deg \hat{M}(x)$.

В работе [5] представлен протокол аутентификации спутника, реализованный в ПМК. Выбираем параметры, удовлетворяющие условию

$$\log_2 \{U, S(j), T(j)\} < \deg \hat{M}(x), \quad (5)$$

где U – секретный ключ спутника, $S(j)$ и $T(j)$ – сеансовый ключ и число, позволяющее определить повторное использование данного ключа.

Представляем их $U = (u_1 \| u_2 \| ... \| u_k)$, $S^j = (S_1^j \| S_2^j \| ... \| S_k^j)$, $T^j = (T_1^j \| T_2^j \| ... \| T_k^j)$, где $u_i = \deg m_i(x)$, $S_i^j = \deg m_i(x)$; $T_i^j = \deg m_i(x)$; $i = 1, 2, ..., k$.

1. Перед j-м сеансом связи ответчик определяет истинный статус спутника в ПМК

$$C^j(x) = (C_1^j(x), C_2^j(x), ..., C_k^j(x)), \quad (6)$$

где $C_i^j(x) = \left|g(x)^{u_i}\, g(x)^{S_i^j}\, g(x)^{T_i^j}\right|^{+}_{m_i(x)}$; $g(x) = x$; $i = 1, 2, ..., k$.

2. Затем производится изменение секретных параметров

$$\tilde{u}_i = (u_i + \Delta u_i) \bmod G_i, \quad \tilde{S}_i^j = (S_i^j + \Delta S_i^j) \bmod G_i, \quad \tilde{T}_i^j = (T_i^j + \Delta T_i^j) \bmod G_i, \quad (7)$$

где $\left\{\Delta u_i, \Delta S_i^j, \Delta T_i^j\right\} < G_i$ – случайные числа; $G_i = 2^{\deg m_i(x)} - 1$; $i = 1, 2, ..., k$.

3. После вычисляется зашумленный статус спутника, используя ПМК

$$\tilde{C}^j(x) = (\tilde{C}_1^j(x), \tilde{C}_2^j(x), ..., \tilde{C}_k^j(x)), \quad (8)$$

где $\tilde{C}_i(x) = \left|g(x)^{\tilde{u}_i}\, g(x)^{\tilde{S}_i^j}\, g(x)^{\tilde{T}_i^j}\right|^{+}_{m_i(x)}$.

4. Для опознавания запросчик задает вопрос $d^j = (d_1^j, d_2^j, ... d_k^j)$, где $d_i^j \equiv d^j \bmod G_i$.

5. Ответчик, находящийся на спутнике, отвечает на вопрос $d^j = (d_1^j, d_2^j, ... d_k^j)$

$$r_i^1 = (\tilde{u}_i - d_i^j \cdot u_i) \bmod G_i, \quad r_i^2 = (\tilde{S}_i^j - d_i^j \cdot S_i^j) \bmod G_i, \quad r_i^3 = (\tilde{T}_i^j - d_i^j \cdot T_i^j) \bmod G_i. \quad (9)$$

6. Ответчик осуществляет передачу запросчику следующих данных

$$\left\{(C_1^j(x),...,C_k^j(x)),(\tilde{C}^j(x),...,\tilde{C}_k^j(x)),(r_1^1,...,r_k^1),(r_1^2,...,r_k^2),(r_1^3,...,r_k^3)\right\}.$$

7. Запросчик осуществляет проверку статуса спутника

$$Y_i^j(x)=\left|\left(C_i^j(x)\right)^{d_i^j}\ g(x)^{r_i^1}\ g(x)^{r_i^2}\ g(x)^{r_i^3}\right|^{+}_{m_i(x)}. \tag{10}$$

Статус «свой» будет только при выполнении условия

$$\left\{\ Y_1^j(x)=\tilde{C}_1^j(x),\ Y_2^j(x)=\tilde{C}_2^j(x),...,\ Y_k^j(x)=\tilde{C}_k^j(x)\right\}. \tag{11}$$

Анализ выражений (5)–(11) показывает, что применение ПМК позволило сократить время опознавания. При этом ПМК способны осуществлять поиск и исправление ошибок [7]. Так, для исправления однократной ошибки необходимо два основания, так чтобы

$$\deg m_{k-1}(x)+\deg m_k(x)\le\deg m_{k+1}(x)+\deg m_{k+2}(x). \tag{12}$$

В результате этого получаем полный диапазон избыточного ПМК

$$M(x)=\prod_{i=1}^{k+2}m_i(x)=\hat{M}(x)\prod_{i=k+1}^{k+2}m_i(x). \tag{13}$$

Комбинация $Y(x)=(y_1(x),\ y_2(x),...,y_{k+2}(x))$ не содержит ошибки, если

$$\deg Y(x)<\deg\hat{M}(x)=\prod_{i=1}^{k}m_i(x). \tag{14}$$

Однократная ошибка изменяет значение j-го остатка согласно

$$Y^*(x)=(y_1(x),,...,\ y_j^*(x),...,y_{k+2}(x))=(y_1(x),,...,\left|y_j(x)\oplus\Delta y_j(x)\right|_{m_i(x)},...,y_{k+2}(x)), \tag{15}$$

где $y_j^*(x)$ – искаженный остаток ПМК; $\Delta y_j(x)$ – глубина однократной ошибки.

В результате нарушается условие (14), так как имеем

$$Y^*(x)=\sum_{\substack{i=1\\ j\ne i}}^{k+2}(y_i(x)B_i(x)=(y_j(x)+\Delta y_j(x))B_j(x))\bmod M(x)=Y(x)+\Delta y_j(x)B_j(x), \tag{16}$$

где $B_i(x)$ – ортогональные базисы ПМК; $B_i(x)=M_i(x)M_i^{-1}(x)$; $M_i(x)=M(x)/m_i(x)$.

Для поиска и коррекции ошибок в полиномиальных модулярных кодах в работе [7] рекомендуется вычислять позиционную характеристику – интервал ПМК

$$\begin{cases}L_{k+1}(x)=\left(\sum\limits_{i=1}^{k+2}y_i(x)C_i(x)+\hat{R}(x))\right)\bmod m_{k+1}(x),\\ L_{k+2}(x)=\left(\sum\limits_{i=1}^{k+2}y_i(x)C_i(x)+\hat{R}(x))\right)\bmod m_{k+2}(x),\end{cases} \tag{17}$$

где $B_i(x)=C_i(x)\hat{M}(x)+\hat{B}_i(x)$; $\hat{B}_j(z)$ и $\hat{R}(x)=\left[\sum\limits_{j=1}^{k}y_j(x)\hat{B}_j(x)\Big/\hat{M}(x)\right]$ – ортогональный базис и ранг кортежа информационных оснований ПМК.

С целью снижения схемных затрат был разработан алгоритм, позволяющий определить место и величину ошибки на основе модульной свертки.

$$\begin{cases} \sigma_1(x) = y_{k+1}(x) \oplus \ddot{y}_{k+1}(x) = y_{k+1}(x) \oplus \left| \sum_{j=1}^{k} \lambda_j(x) y_j(x) \right|^{+}_{m_{k+1}(x)} \\ \sigma_2(x) = y_{k+2}(x) \oplus \ddot{y}_{k+2}(x) = y_{k+2}(x) \oplus \left| \sum_{j=1}^{k} \lambda_j(x) y_j(x) \right|^{+}_{m_{k+2}(x)} \end{cases}, \quad (18)$$

где $\ddot{y}_{k+s}(x) = \left| \sum_{j=1}^{k} \lambda_j(x) z_j(x) \right|^{+}_{m_{k+s}(x)}$ – модульная свертка; $\lambda_j(x)$ – константа свертки; s = 1,2.

Для вычисления констант модульной свертки воспользуемся китайской теоремой об остатках (КТО) для безызбыточной системы полиномиального модулярного кода, то есть

$$Y(x) = \left(\sum_{j=1}^{k} y_j(x) \hat{B}_j(x) \right) \bmod \hat{M}(x) = \sum_{j=1}^{k} y_j(x) \hat{B}_j(x) - \hat{R}(x) \hat{M}(x). \quad (19)$$

Известно, что ортогональный базис определяется

$$\hat{B}_j(x) = M_j^{-1}(x) M_j(x) = M_j^{-1}(x) \hat{M}(x) \big/ m_j(x), \quad (20)$$

где $M_j^{-1}(x)$ – вес ортогонального базиса.

Чтобы определить константу свертки $z_j(x)\lambda_j(x)$, где j = 1, 2, ..., k, необходимо найти $z_j(x) = y_j(x) M_j^{-1}(x) \bmod m_j(x)$, при этом $\deg\left(y_j(x) M_j^{-1}(x) \bmod m_j(x) \right) < \deg m_j(x)$ В этом случае при реализации (19) можно отказаться от вычисления ранга, то есть имеем

$$Y(x) = \sum_{j=1}^{k} \left| y_j(x) M_j^{-1}(x) \right|^{+}_{m_j(x)} M_j(x). \quad (21)$$

Тогда $z_j(x)\lambda_j(x) \bmod m_{k+s}(x)$, где j = 1, 2, ..., k, s = 1, 2., определяется

$$z_j(x)\lambda_j(x) \bmod m_{k+s}(x) = \left(\left| y_j(x) M_j^{-1}(x) \right|^{+}_{m_j(x)} M_j(x) \right) \bmod m_{k+s}(x). \quad (22)$$

Значит, модульная свертка позволяет корректировать ошибку в ПМК, используя

$$\begin{cases} \sigma_1(x) = y_{k+1}(x) \oplus \left| \sum_{j=1}^{k} \left| M_j^{-1}(x) y_j(x) \right|^{+}_{m_j(x)} M_j(x) \right|^{+}_{m_{k+1}(x)} \\ \sigma_2(x) = y_{k+2}(x) \oplus \left| \sum_{j=1}^{k} \left| M_j^{-1}(x) y_j(x) \right|^{+}_{m_j(x)} M_j(x) \right|^{+}_{m_{k+2}(x)} \end{cases} \quad (23)$$

Если свертка $\ddot{y}_{k+s}(x) = \left| \sum_{j=1}^{k} \lambda_j(x) z_j(x) \right|^{+}_{m_{k+s}(x)}$ совпадает с контрольным основанием, то комбинация ПМК не содержит ошибки. В противном случае – комбинация ПМК ошибочная.

Результаты исследования и их обсуждение

В качестве информационных оснований ПМК выбираем $m_1(x)=x^5+x^4+x^3+x+1$, $m_2(x)=x^5+x^4+x^3+x^2+1$, $m_3(x)=x^5+x^3+x^2+x+1$. Согласно (1) рабочий диапазон $\hat{M}(x)=\prod_{i=1}^{3}m_i(x)=x^{15}+x^{11}+x^{10}+x^2+1$. Согласно (12) контрольными основаниями ПМК будут $m_4(x)=x^5+x^2+1$ и $m_5(x)=x^5+x^3+1$. Используя (21), определим

$$M_1(x)=m_2(x)m_3(x)=x^{10}+x^9+x^7+x^6+x^5+x^4+x^3+x+1;\ M_1^{-1}(x)=x^4+x^2+1;$$
$$M_2(x)=m_1(x)m_3(x)=x^{10}+x^9+x^4+x^3+1;\ M_2^{-1}(x)=x^4+x+1;$$
$$M_3(x)=m_1(x)m_2(x)=x^{10}+x^8+x^7+x^6+x^4+x^3+x^2+x+1;\ M_3^{-1}(x)=x^2+x+1.$$

Для выполнения алгоритма поиска и коррекции ошибки вычислим константы

$$\lambda_1(x)\bmod m_4(x)=\left|M_1(x)\right|^{+}_{m_4(x)}=\left|x^{10}+x^9+x^7+x^6+x^5+x^4+x^3+x+1\right|^{+}_{m_4(x)}=x^3+x+1;$$
$$\lambda_2(x)\bmod m_4(x)=\left|M_2(x)\right|^{+}_{m_4(x)}=\left|x^{10}+x^9+x^4+x^3+1\right|^{+}_{m_4(x)}=x^4+x;$$
$$\lambda_3(x)\bmod_4(x)=\left|M_3(x)\right|^{+}_{m_4(x)}=\left|x^{10}+x^8+x^7+x^6+x^4+x^3+x^2+x+1\right|_{m_4(x)}=x^4+x^3+x^2+1.$$

Для второго контрольного основания $m_2(x)=x^5+x^3+1$ имеем константы

$$\lambda_1(x)\bmod m_5(x)=\left|M_1(x)\right|^{+}_{m_5(x)}=\left|x^{10}+x^9+x^7+x^6+x^5+x^4+x^3+x+1\right|^{+}_{m_5(x)}=x+1;$$
$$\lambda_2(x)\bmod m_5(x)=\left|M_2(x)\right|^{+}_{m_5(x)}=\left|x^{10}+x^9+x^4+x^3+1\right|^{+}_{m_5(x)}=x^4+x^2+x+1;$$
$$\lambda_3(x)\bmod_5(x)=\left|M_3(x)\right|^{+}_{m_5(x)}=\left|x^{10}+x^8+x^7+x^6+x^4+x^3+x^2+x+1\right|_{m_5(x)}=x^3+1.$$

Выбираем $Y(x)=x^7+x+1=(x^4+x^3+1,x^3+x^2+1,x^4,x^4+x^2+x+1,x^3+x^2+x)$. Вычислим произведение $z_j(x)=y_j(x)M_j^{-1}(x)\bmod m_j(x)$, где j = 1, 2, 3. Тогда

$$z_1(x)=y_1(x)M_1^{-1}(x)\bmod m_1(x)=\left|(x^4+x^3+1)(x^4+x^2+1)\right|^{+}_{x^5+x^4+x^3+x+1}=x^3+x^2+x,$$
$$z_2(x)=y_2(x)M_2^{-1}(x)\bmod m_2(x)=\left|(x^3+x^2+1)(x^4+x+1)\right|^{+}_{x^5+x^4+x^3+x^2+1}=x^3+x^2+x,$$
$$z_3(x)=y_3(x)M_3^{-1}(x)\bmod m_3(x)=\left|x^4\cdot(x^2+x+1)\right|^{+}_{x^5++x^3+x^2+x+1}=1.$$

Воспользуемся модульной сверткой и вычислим контрольные остатки

$$\ddot{y}_4(x)=\left|\sum_{j=1}^{3}\lambda_j(x)z_j(x)\right|^{+}_{m_4(x)}=((x^3+x^2+x)(x^3+x+1)+(x^3+x^2+x)(x^4+x)+$$
$$+(x^4+x^3+x^2+1))\bmod x^5+x^2+1=x^4+x^2+x+1,$$
$$\ddot{y}_5(x)=\left|\sum_{j=1}^{3}\lambda_j(x)z_j(x)\right|^{+}_{m_5(x)}=((x^3+x^2+x)(x+1)+(x^3+x^2+x)(x^4+x^2+x+1)+$$
$$+(x^3+1))\bmod x^5+x^3+1=x^3+x^2+x.$$

Тогда согласно (18) получаем, что комбинация не содержит ошибки, так как

$$\begin{cases}\sigma_1(x) = y_{k+1}(x) + \ddot{y}_{k+1}(x) = (x^4 + x^2 + x + 1) + (x^4 + x^2 + x + 1) = 0, \\ \sigma_2(x) = y_{k+2}(x) + \ddot{y}_{k+2}(x) = (x^3 + x^2 + x) + (x^3 + x^2 + x) = 0.\end{cases}$$

Введем ошибку, равную $\Delta y_2(x) = x + 1$. Тогда $y_2^*(x) = \left| y_2(x) + \Delta y_2(x) \right|_{m_2(x)}^{+} = x^2 + x$, а комбинация ПМК примет вид $Y^*(x) = (x^4 + x^3 + 1, x^3 + x^2 + x, x^4, x^4 + x^2 + x + 1, x^3 + x^2 + x)$. Вычислим остатки по контрольным основаниям

$$z_2^*(x) = y_2(x) M_2^{-1}(x) \bmod m_2(x) = \left| (x^3 + x^2 + x)(x^4 + x + 1) \right|_{x^5 + x^4 + x^3 + x^2 + 1}^{+} = x^2 + x\,.$$

Воспользуемся модульной сверткой и вычислим контрольные остатки

$$\ddot{y}_4^*(x) = \left| \sum_{j=1}^{3} \lambda_j(x) z_j(x) \right|_{m_4(x)}^{+} = ((x^3 + x^2 + x)(x^3 + x + 1) + (x^2 + x)(x^4 + x) + (x^4 + x^3 + x^2 + 1)) \bmod x^5 + x^2 + 1 = x^4 + 1,$$

$$\ddot{y}_5^*(x) = \left| \sum_{j=1}^{3} \lambda_j(x) z_j(x) \right|_{m_5(x)}^{+} = ((x^3 + x^2 + x)(x + 1) + (x^2 + x)(x^4 + x^2 + x + 1) + (x^3 + 1)) \bmod x^5 + x^3 + 1 = x^4 + x.$$

Тогда согласно (18) получаем, что комбинация содержит ошибки, так как

$$\begin{cases}\sigma_1(x) = y_{k+1}(x) + \ddot{y}_{k+1}^*(x) = (x^4 + x^2 + x + 1) + (x^4 + 1) = x^2 + x, \\ \sigma_2(x) = y_{k+2}(x) + \ddot{y}_{k+2}^*(x) = (x^3 + x^2 + x) + (x^4 + x) = x^4 + x^3 + x^2.\end{cases}$$

На основании результата выбираем вектор ошибки $\overline{e}(x) = (0, x + 1, 0, 0, 0)$. Тогда

$$Y(x) = Y^*(x) + \overline{e}(x) = (x^4 + x^3 + 1, x^3 + x^2 + 1, x^4, x^4 + x^2 + x + 1, x^3 + x^2 + x)\,.$$

Используя рассмотренный алгоритм, разработали структурную схему устройства поиска и коррекции ошибки. Произведем оценку схемных затрат на реализацию разработанного алгоритма. Устройство содержит два тракта, в каждом из которых:

– три LUT-таблицы, реализующие вычисление $z_j(x) = y_j(x) M_j^{-1}(x) \bmod m_j(x)$;

– три LUT-таблицы, реализующие вычисление $z_j(x) \lambda_j(x) \bmod m_{k+s}(x)$;

– две LUT-таблицы, реализующие вычисление модульной свертки.

Значит, на устройство поиска и коррекции ошибки, использующее модульную свертку, необходимо 16 LUT-таблиц.

В этом случае устройство, реализующее алгоритм поиска и коррекции ошибок, определяемый (14), также содержит два тракта, в каждом из которых:

– пять LUT-таблиц, реализующих вычисление $s_i(x) = \left| y_i(x) C_i(x) \right|_{m_i(x)}^{+}$;

– четыре LUT-таблицы, реализующие вычисление ранга ПМК;

– три LUT-таблицы, реализующие вычисление $\sum_{i=1}^{5} y_i(x) C_i(x) + \hat{R}(x))$.

Значит, на устройство поиска и коррекции ошибки, построенное на основе алгоритма [7], необходимо 22 LUT-таблицы. Таким образом, разработанный алгоритм позволяет сократить аппаратные затраты в 1,375 раза по сравнению с использованием алгоритма вычисления интервала ПМК.

Заключение

С целью сокращения времени, необходимого на определение статуса космического аппарата, был предложен протокол аутентификации, реализованный в ПМК. При этом полиномиальные модулярные коды позволяют обнаруживать и исправлять ошибки, которые возникают в процессе функционирования системы опознавания,

что позволит повысить ее отказоустойчивость. В работе показан алгоритм поиска и коррекции ошибок в полиномиальных кодах, который базируется на использовании модульной свертки. Проведенные исследования показали, что при использовании полиномов пятой степени разработанный алгоритм требует в 1,375 раза меньше аппаратных затрат по сравнению с алгоритмом вычисления интервала ПМК, приведенным в работе [7].

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

Список литературы

1. Камнев В.Е., Черкасов В.В., Чечин Г.В. Спутниковые сети связи. М.: «Альпина Паблишер», 2015. 489 с.

2. Кукк К.И. Спутниковая связь: прошлое, настоящее, будущее. М.: Горячая линия – Телеком, 2017. 256 с.

3. Rezenkov R.N., Pashintsev V.P., Zhuk P.A. Application of spoof resistant authentication protocol of spacecraft in low earth orbit systems of satellite communication. International Journal of Mechanical Engineering and Technology (IJMET). 2018.Vol. 9. Issue 5, May. P. 958–965.

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

5. Pashintsev V.P., Zhuk F.P., Chistousov N.K. Development of Satellite Authentication System for Low Earth Orbit Satellite Communication System on the Basis of Polynomial Residue Number System. International Journal of Engineering and Advanced Technology (IJEAT). 2019. Vol. 8 Issue 5. P. 2557–2562.

6. Калмыков И.А. Емарлукова Я.В. Математические модели и схемные решения отказоустойчивых непозиционных вычислительных систем: монография. Ставрополь: Изд-во СКФУ, 2016. 216 с.

7. Горденко Д.В., Резеньков Д.Н., Саркисов А.Б. Методы и алгоритмы реконфигурации непозиционных вычислительных структур для обеспечения отказоустойчивости спецпроцессоров. Ставрополь: Издательство Фабула, 2014. 180 с.