УДК 004.052.2

АЛГОРИТМ КОРРЕКЦИИ ОШИБОК, ВОЗНИКАЮЩИХ ПРИ ВЫЧИСЛЕНИИ ОТВЕТА НА ЗАПРОС ОТКАЗОУСТОЙЧИВОЙ СИСТЕМЫ ОПОЗНАВАНИЯ СПУТНИКА

Калмыков И.А., Чипига А.Ф., Калмыкова Н.И., Чистоусов Н.К.

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

Для организации связи с необслуживаемыми объектами, используемыми для добычи углеводородов, месторождения которых находятся за Полярным кругом, широко применяются низкоорбитальные системы спутниковой связи. Одним из решений, позволяющих повысить их информационную скрытность, является использование системы опознавания спутника. Применение протокола аутентификации, реализованного в полиномиальных модулярных кодах (ПМК), позволяет перед началом сеанса связи определить статус спутника при минимальных временных затратах. Данный результат достигается за счет параллельных вычислений, выполняемых с помощью ПМК. Однако полиномиальные модулярные коды способны осуществлять поиск и исправление ошибок. Данные ошибки могут появляться из-за отказов и сбоев вычислительных устройств системы опознавания. В классическом подходе для повышения отказоустойчивости в систему, функционирующую в ПМК, вводят дополнительные контрольные основания. Однако это может привести к снижению имитостойкости протокола, так как все остатки ПМК несут информацию о числе, которое представляется в этом коде. Поэтому необходимо разработать такой алгоритм поиска и коррекции ошибок в ПМК, в котором проверочные остатки представляли бы собой результат свертки, полученной с использованием информационных остатков. Цель работы – обеспечить возможность поиска и коррекции ошибок, возникающих при вычислении ответа на «вопрос» запросчика, на основе разработанного алгоритма.

Ключевые слова: система аутентификации спутника, полиномиальные модулярные коды, алгоритмы поиска и коррекции ошибок в модулярном коде

ALGORITHM FOR CORRECTING ERRORS THAT OCCUR WHEN CALCULATING THE RESPONSE TO A REQUEST FOR A FAULT-TOLERANT SATELLITE IDENTIFICATION SYSTEM

Kalmykov I.A., Chipiga A.F., Kalmykova N.I., Chistousov N.K.

North-Caucasian Federal University, Stavropol, e-mail: kia762@yandex.ru

Low-orbit satellite communication systems are widely used for organizing communications with non-maintenance facilities used for the production of hydrocarbons whose deposits are located beyond the Arctic Circle. One of the solutions to increase their information secrecy is the use of a satellite identification system. Using the authentication Protocol implemented in polynomial modular codes (PMC) allows you to determine the satellite status before starting a communication session with minimal time spent. This result is achieved by parallel calculations performed with the help of PMC. However, polynomial modular codes are capable of searching for and correcting errors. These errors may occur due to failures and failures of the identification system's computing devices. In the classic approach, additional control grounds are introduced into the system that functions in the PMK to increase fault tolerance. However, this can lead to a decrease in the Protocol's imitability, since all the remaining PMCs carry information about the number that is represented in this code. Therefore, it is necessary to develop an algorithm for searching and correcting errors in the PMK, in which the verification balances would be the result of a convolution, obtained using information balances. The purpose of this work is to provide the ability to search for and correct errors that occur when calculating the answer to the «question» of the requester, based on the developed algorithm.

Keywords: satellite authentication system, polynomial modular codes, algorithms for searching and correcting errors in the modular code

Освоение месторождений в районах прибрежной зоны Северного Ледовитого океана невозможно без использования низкоорбитальных систем спутниковой связи (НССС). Так как высота орбиты не превышает 1500 км, то для организации бесперебойной связи необходима группировка, в состав которой входит не менее 60 спутников [1, 2]. По мере увеличения числа НССС, используемых компаниями при освоении недр Крайнего Севера, возрастает вероятность навязывания перехваченной и задержанной команды, предназначенной для управления необслуживаемым объектом добычи углеводородов. В результате этого может возникнуть экологическая катастрофа.

Для предотвращения навязывания ретрансляционной помехи и повышения помехозащищенности НССС в работах [3, 4] предлагается развертывать на борту спутников систему опознавания «свой – чужой». При этом для уменьшения времени, необходимого на вычисление статуса спутника, в работах [5, 6] был разработан протокол аутентификации, который был выполнен с использованием полиномиальных модулярных кодов (ПМК). Известно,

что введение дополнительных оснований в ПМК позволяет проводить процедуры поиска и исправления ошибок, возникающих в процессе вычислений. Таким образом, использование ПМК позволит повысить отказоустойчивость системы опознавания, что является одной из наиболее важных задач. Однако применение известных алгоритмов обнаружения и коррекции ошибок в полиномиальных модулярных кодах может привести к снижению криптостойкости системы опознавания, так как контрольные остатки предоставляют дополнительную информацию о числе, представленном в ПМК. Поэтому разработка алгоритма поиска и коррекции ошибок в ПМК, в котором проверочные остатки представляли бы собой результат свертки, полученной с использованием информационных остатков, является актуальной задачей.

В основу работы системы опознавания спутника положен протокол аутентификации типа «запрос – ответ», обладающий нулевым разглашением сведений. В данном протоколе претендент с помощью ответа на поставленный вопрос должен доказать проверяющей стороне, что он относится к авторизованным абонентам. При этом его ответ должен зависеть как вопроса, так и от секретных сведений, которые известны только ему. Очевидно, что ошибки, которые могут возникнуть из-за отказа оборудования ответчика, расположенного на борту спутника, приведут к искажению ответа. В результате этого проверяющая сторона воспримет спутник как «чужой» и не предоставит ему сеанс связи. Поэтому целью работы является обеспечение возможности коррекции ошибочного ответа на «вопрос» запросчика на основе разработанного алгоритма поиска и коррекции ошибок в ПМК.

Материалы и методы исследования

Полиномиальные модулярные коды относятся к группе непозиционных кодов [7, 8]. В таких кодах полином $Z(x)$, полученный из двоичного числа Z, заменяется кортежем остатков

$$Z(x) = (z_1(x), z_2(x), ..., z_k(x)), \quad (1)$$

где $z_i(x) \equiv Z(x) \bmod p_i(x)$, $i = 1, 2, ..., k$.

Из равенства (1) видно, что остатки получаются при делении многочлена $Z(x)$ на основания, в качестве которых выбраны неприводимые многочлены $p_i(x)$, которые определяют рабочий диапазон ПМК

$$P(x) = \prod_{i=1}^{k} p_i(x). \quad (2)$$

Использование ПМК позволяет эффективно выполнять модульные операции вида

$$\left|Z(x) + W(x)\right|^{+}_{P(x)} = ((z_1(x) + w_1(x)) \bmod p_1(x), ..., (z_k(x) \oplus w_k(x)) \bmod p_k(x)), \quad (3)$$

$$\left|Z(x) \cdot W(x)\right|^{+}_{P(x)} = ((z_1(x) \cdot w_1(x)) \bmod p_1(x), ..., (z_k(x) \cdot w_k(x)) \bmod p_k(x)), \quad (4)$$

где $w_i(x) \equiv W(x) \bmod p_i(x)$; $i = 1, 2, ..., k$.

В работе [6] представлен протокол аутентификации с нулевым разглашением, который реализуется на основе ПМК. На его предварительном этапе определяются порождающий элемент $g = x$, значения секретного ключа спутника K, сеансового ключа для j-го сеанса $S(j)$, дополнительного параметра проверки $T(j)$, из условия

$$\log_2 \{K, S(j), T(j)\} < \deg P(x), \quad (5)$$

где $\deg P(x)$ – степень многочлена $P(x)$, определяемого равенством (2).

Учитывая разрядность оснований МПК, выбираются блоки $K_i = \deg p_i(x)$, $S_i^j = \deg p_i(x)$, $T_i^j = \deg p_i(x)$, где $i = 1, 2, ..., k$. Это позволяет получить следующие результаты

$$K = (K_1 \| K_2 \| ... \| K_k), \; S^j = (S_1^j \| S_2^j \| ... \| S_k^j), \; T^j = (T_1^j \| T_2^j \| ... \| T_k^j), \quad (6)$$

На первом этапе протокола ответчиком производится вычисление истинного статуса

$$C^j(x) = \left(\left| g(x)^{K_1} g(x)^{S_1^j} g(x)^{T_1^j} \right|^{+}_{p_i(x)}, ..., \left| g(x)^{K_k} g(x)^{S_k^j} g(x)^{T_k^j} \right|^{+}_{p_i(x)} \right). \quad (7)$$

На втором этапе ответчиком производится определение «зашумленных» параметров. На основе сгенерированных чисел $\left\{\Delta K_i, \Delta S_i^j, \Delta T_i^j\right\} < L$, где $L = 2^{\deg p_i(x)} - 1$, получаются

$$\tilde{K}_i^j = \left|K_i + \Delta K_i^j\right|_L^+, \ \tilde{S}_i^j = \left|S_i^j + \Delta S_i^j\right|_L^+, \ \tilde{T}_i^j = \left|T_i^j + \Delta T_i^j\right|_L^+. \quad (8)$$

На третьем этапе ответчик получает значение «зашумленного» статуса борта

$$\tilde{C}^j(x) = \left(\left|g(x)^{\tilde{K}_1^j} g(x)^{\tilde{S}_1^j} g(x)^{\tilde{T}_1^j}\right|_{p_i(x)}^+, ..., \left|g(x)^{\tilde{K}_k} g(x)^{\tilde{S}_k^j} g(x)^{\tilde{T}_k^j}\right|_{p_i(x)}^+\right). \quad (9)$$

На четвертом этапе запросчик генерирует случайное число-вопрос $d^j = (d_1^j, d_2^j, ... d_k^j)$, где $d_i^j \equiv d^j \bmod L$, $L = 2^{\deg p_i(x)} - 1$, $i = 1, 2, ..., k$, которое передается на борт спутника.

На пятом этапе ответчик, используя выражения (3) и (4), вычисляет ответы на вопрос

$$r_i^1(j) = \left|\tilde{K}_i^j - d_i^j - K_i^j\right|_L^+, \ r_i^2(j) = \left|\tilde{S}_i^j - d_i^j - S_i^j\right|_L^+, \ r_i^3(j) = \left|\tilde{T}_i^j - d_i^j - T_i^j\right|_L^+. \quad (10)$$

Тогда ответный сигнал спутника имеет вид

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

На шестом этапе процесса аутентификации запросчик проверяет ответы

$$Y_i^j(x) = \left|C_i^j(x) g(x)^{r_i^1} g(x)^{r_i^2} g(x)^{r_i^3} g^{3d_i}\right|_{p_i(x)}^+. \quad (11)$$

Космический аппарат получит статус «свой», при выполнении выражения

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

Очевидно, что аутентификация спутника в первую очередь зависит от правильности ответов на вопросы запросчика, которые вычисляются на борту спутника. В рассмотренном протоколе ответы $r_i^1(j), r_i^2(j), r_i^3(j)$ вычисляются по одному модулю $L = 2^{\deg p_i(x)} - 1$. Значит, классические алгоритмы поиска и коррекции ошибок в модулярных кодах применять нельзя. Устранить данный недостаток позволяет разработанный алгоритм взвешенной свертки кода, в котором для коррекции ошибки в одном остатке вычисляются два контрольных остатка

$$r_{k+1}(j) = \sum_{i=1}^{k} r_i(j) \bmod 2_i^{\deg p_i(x)} - 1,$$

$$r_{k+2}(j) = \sum_{i=1}^{k} 2^{i-1} r_i(j) \bmod 2_i^{\deg p_i(x)} - 1, \quad (12)$$

где $R(j) = (r_1(j), r_2(j), ..., r_k(j))$, – ответ на j-й вопрос.

Результаты исследования и их обсуждение

Пусть в ПМК выбраны модули $p_1(x) = x^5 + x^4 + x^3 + x + 1$, $p_2(x) = x^5 + x^4 + x^3 + x^2 + 1$, $p_3(x) = x^5 + x^3 + x^2 + x + 1$. Тогда диапазон $P(x) = \prod_{i=1}^{3} p_i(x) = x^{15} + x^{11} + x^{10} + x^2 + 1$. Из условия (5) выбираем секретный ключ $K = 31063$, параметры $S = 12002$, $T = 24001$. Воспользуемся выражением (6) и представим их в двоичном коде, который разобьем на блоки по 5 бит.

$K = 31063 = 111100101010111_2 = 11110\ 01010\ 10111 = 30_{10} \| \ 10_{10} \| 23_{10} = K_1 \| \ K_2 \| \ K_3.$

$S = 12002 = 010\ 1110\ 1110\ 0010_2 = 01011\ 10111\ 00010 = 11_{10} \| \ 23_{10} \| 2_{10} = S_1 \| \ S_2 \| \ S_3.$

$T = 24001 = 101\ 1101\ 1100\ 0001_2 = 10111\ 01110\ 00001 = 23_{10} \| \ 14_{10} \| 1_{10} = T_1 \| \ T_2 \| \ T_3.$

1. Определение истинного статуса космического аппарата согласно (7)

$$C_1^j(x) = \left| g(x)^{K_1}\, g(x)^{S_1^j}\, g(x)^{T_1^j} \right|_{p_1(x)}^{+} = \left| x^{30} \cdot x^{11} \cdot x^{23} \right|_{p_1(x)}^{+} = \left| x^{2} \right|_{p_1(x)}^{+} = 00100 = 4,$$

$$C_2^j(x) = \left| x^{10} \cdot x^{23} \cdot x^{14} \right|_{p_2(x)}^{+} = \left| x^{16} \right|_{p_2(x)} = 01011 = 11,$$

$$C_3^j(x) = \left| x^{23} \cdot x^{2} \cdot x^{1} \right|_{p_3(x)}^{+} = \left| x^{26} \right|_{p_3(x)}^{+} = 10100 = 20.$$

2. Для определения «зашумленных» параметров воспользуемся равенствами (8). Тогда при выбранных $\Delta K = 3332, \Delta S = 10353, \Delta T = 2441$ получаем

$$\tilde{K}^j = \left(\left| 30+3 \right|_{31}^{+} \| \left| 10+8 \right|_{31}^{+} \| \left| 23+4 \right|_{31}^{+} \right) = \left(2 \| 18 \| 27 \right) = \left(\tilde{K}_1 \| \tilde{K}_2 \| \tilde{K}_3 \right),$$

$$\tilde{S}^j = \left(\left| 11+10 \right|_{31}^{+} \| \left| 23+3 \right|_{31}^{+} \| \left| 17+2 \right|_{31}^{+} \right) = \left(21 \| 26 \| 19 \right) = \left(\tilde{S}_1 \| \tilde{S}_2 \| \tilde{S}_3 \right),$$

$$\tilde{T}^j = \left(\left| 23+2 \right|_{31}^{+} \| \left| 14+12 \right|_{31}^{+} \| \left| 1+9 \right|_{31}^{+} \right) = \left(25 \| 26 \| 10 \right) = \left(\tilde{T}_1 \| \tilde{T}_2 \| \tilde{T}_3 \right).$$

3. Определение «зашумленного» статуса космического аппарата согласно (9)

$$\tilde{C}_1^j(x) = \left| g(x)^{\tilde{K}_1}\, g(x)^{\tilde{S}_1^j}\, g(x)^{\tilde{T}_1^j} \right|_{p_i(x)}^{+} = \left| x^{2} \cdot x^{21} \cdot x^{25} \right|_{p_1(x)}^{+} = \left| x^{17} \right|_{p_1(x)} = 01011_2 = 11,$$

$$\tilde{C}_2^j(x) = \left| x^{18} \cdot x^{26} \cdot x^{26} \right|_{p_2(x)}^{+} = \left| x^{8} \right|_{p_2(x)} = 11100 = 28,$$

$$\tilde{C}_3^j(x) = \left| x^{27} \cdot x^{19} \cdot x^{10} \right|_{p_3(x)}^{+} = \left| x^{25} \right|_{p_3(x)} = 01010 = 10.$$

4. Запросчик передает число-вопрос $d^j = 00111 \| 00100 \| 10110 = 7 \| 4 \| 22$.

5. Ответчик определяет ответы на поставленный вопрос, используя выражения (10). Тогда для первого модуля имеем

$$r_1^1(j) = \left| \tilde{K}_1^j - d_1^j - K_1 \right|_{31}^{+} = 27,\ r_1^2(j) = \left| 21-7-11 \right|_{31}^{+} = 3,\ r_1^3(j) = \left| 25-7-23 \right|_{31}^{+} = 26.$$

Для второго основания ответы на вопрос будут определяться как

$$r_2^1(j) = \left| \tilde{K}_2 - d_2^j - K_2 \right|_{31}^{+} = 4,\ r_2^2(j) = \left| 26-4-23 \right|_{31}^{+} = 30,\ r_2^3(j) = \left| 26-4-14 \right|_{31}^{+} = 8.$$

Для третьего основания ответы на вопрос будут определяться как

$$r_3^1(j) = \left| \tilde{K}_3^j - d_3^j \cdot K_3 \right|_{31}^{+} = 13,\ r_3^2(j) = \left| 19-22-2 \right|_{31}^{+} = 26,\ r_3^3(j) = \left| 10-22-1 \right|_{31}^{+} = 18.$$

Ответчик осуществляет передачу двух статусов и ответов представленных ПМК.

6. Запросчик, используя выражение (11), определяет статус спутника

$$Y_1^j(x) = \left| x^{2} \cdot x^{27} \cdot x^{3} \cdot x^{26} \cdot x^{7\cdot 3} \right|_{p_1(x)}^{+} = \left| x^{17} \right|_{p_1(x)}^{+} = 01011,$$

$$Y_2^j(x) = \left| (x^3+x+1) x^4 x^{30} x^8 x^{12} \right|_{p_2(x)}^{+} = 11100,\ Y_3^j(x) = \left| \left(x^4 + x^2 \right) x^{17} x^6 x^{19} x^{66} \right|_{p_3(x)}^{+} = 01010.$$

Так как $\left\{ Y_i^j(x) = \tilde{C}_i^j(x) \right\}$, то спутник получает статус «свой».

Рассмотрим реализацию алгоритма коррекции ошибок, определяемого равенствами (12). Для этого вычислим два контрольных остатка вопроса $d^j = (7, 4, 22)$. Получаем

$$d_4^j = \left|\sum_{i=1}^{3} d_i^j\right|_{31}^{+} = |7+4+22|_{31}^{+} = 2,\ d_5^j = \left|\sum_{i=1}^{3} 2^{i-1} d_i^j\right|_{31}^{+} = |7+2\cdot 4+4\cdot 22|_{31}^{+} = 10.$$

Вычислим два контрольных остатка для секретного ключа $K_j = (30, 10, 23)$. Получаем

$$K_4^j = \left|\sum_{i=1}^{3} K_i^j\right|_{31}^{+} = |30+10+23|_{31}^{+} = 1,\ K_5^j = \left|\sum_{i=1}^{3} 2^{i-1} K_i^j\right|_{31}^{+} = |20+2\cdot 10+4\cdot 23|_{31}^{+} = 18.$$

Вычислим два контрольных остатка для параметра $S^j = (11, 23, 2)$. Получаем

$$S_4^j = \left|\sum_{i=1}^{3} S_i^j\right|_{31}^{+} = |11+23+2|_{31}^{+} = 5,\ S_5^j = \left|\sum_{i=1}^{3} 2^{i-1} S_i^j\right|_{31}^{+} = |11+2\cdot 23+4\cdot 2|_{31}^{+} = 3.$$

Вычислим два контрольных остатка для $T^j = (23, 14, 1)$. Получаем

$$T_4^j = \left|\sum_{i=1}^{3} T_i^j\right|_{31}^{+} = |23+14+1|_{31}^{+} = 7,\ T_5^j = \left|\sum_{i=1}^{3} 2^{i-1} T_i^j\right|_{31}^{+} = |23+2\cdot 14+4\cdot 1|_{31}^{+} = 24.$$

Аналогичным образом получаем

$$\tilde{K}^j = (2, 18, 27, 16, 22),\ \tilde{S}^j = (21, 26, 19, 6, 27),\ \tilde{T}^j = (25, 26, 10, 30, 24).$$

Тогда получаем значения ответов на вопрос $d^j = (7, 4, 22, 2, 10)$.

$$r^1(j) = \left|\tilde{K}^j - d^j - K^j\right|_L^{+} = (2, 18, 27, 16, 22) - (7, 4, 22, 12, 10) - (30, 10, 23, 1, 18) = (27, 14, 13, 13, 25).$$

$$r^2(j) = \left|\tilde{S}^j - d^j - S^j\right|_{31}^{+} = (5, 30, 26, 30, 14),\ r^3(j) = \left|\tilde{T}^j - d^j - T^j\right|_{31}^{+} = (26, 8, 18, 21, 21).$$

Вычислим контрольные остатки по значениям информационных вычетов. Тогда

$$\ddot{r}_4^1(j) = |27+14+13|_{31}^{+} = 13,\ \ddot{r}_5^1(j) = \left|\sum_{i=1}^{3} 2^{i-1} d_i^j\right|_{31}^{+} = |27+2\cdot 14+4\cdot 13|_{31}^{+} = 25.$$

$$\ddot{r}_4^2(j) = |5+30+26|_{31}^{+} = 30,\ \ddot{r}_5^2(j) = \left|\sum_{i=1}^{3} 2^{i-1} d_i^j\right|_{31}^{+} = |5+2\cdot 30+4\cdot 26|_{31}^{+} = 14.$$

$$\ddot{r}_4^3(j) = |26+8+18|_{31}^{+} = 21,\ \ddot{r}_5^3(j) = \left|\sum_{i=1}^{3} 2^{i-1} d_i^j\right|_{31}^{+} = |26+2\cdot 8+4\cdot 18|_{31}^{+} = 21.$$

В этом случае получаем синдром ошибки

$$\sigma_4^1(j) = \left|r_4^1(j) - \ddot{r}_4^1(j)\right|_{31}^{+} = |13-13|_{31}^{+} = 0,\ \sigma_5^1(j) = \left|r_5^1(j) - \ddot{r}_5^1(j)\right|_{31}^{+} = |25-25|_{31}^{+} = 0.$$

$$\sigma_4^2(j) = \left|r_4^2(j) - \ddot{r}_4^2(j)\right|_{31}^{+} = |30-30|_{31}^{+} = 0,\ \sigma_5^2(j) = \left|r_5^2(j) - \ddot{r}_5^2(j)\right|_{31}^{+} = |14-14|_{31}^{+} = 0.$$

$$\sigma_4^3(j) = \left|r_4^3(j) - \ddot{r}_4^3(j)\right|_{31}^{+} = |21-21|_{31}^{+} = 0,\ \sigma_5^3(j) = \left|r_5^3(j) - \ddot{r}_5^3(j)\right|_{31}^{+} = |21-21|_{31}^{+} = 0.$$

Так как синдром ошибки равен нулю, то это означает, что ответы не содержат ошибку. Пусть ошибка глубиной $\Delta K_1^j = 29$ произошла при считывании зашумленного образа ключа. Значит, ошибочный остаток равен $K_1^j = \left|K_1^j + \Delta K_1^j\right|_{31}^+ = \left|30+29\right|_{31}^+ = 28^*$. Тогда

$$\hat{r}^1(j) = (2, 18, 27, 16, 22) - (7, 4, 22, 12, 10) - (28^*, 10, 23, 1, 18) = (25^*, 14, 13, 13, 25).$$

Вычислим контрольные остатки по значениям информационных вычетов. Тогда

$$\ddot{r}_4^1(j) = \left|25+14+13\right|_{31}^+ = 11, \ddot{r}_5^1(j) = \left|\sum_{i=1}^{3} 2^{i-1} d_i^j\right|_{31}^+ = \left|25+2\cdot 14+4\cdot 13\right|_{31}^+ = 23.$$

Тогда синдром ошибки для первого ответа равен

$$\sigma_4^1(j) = \left|\hat{r}_4^1(j) - \ddot{r}_4^1(j)\right|_{31}^+ = \left|13-11\right|_{31}^+ = 2,\ \sigma_5^1(j) = \left|\hat{r}_5^1(j) - \ddot{r}_5^1(j)\right|_{31}^+ = \left|25-23\right|_{31}^+ = 2.$$

Так как синдромы ошибки совпали, то это свидетельствует о том, что ошибка произошла в первом остатке, а ее вектор $\overline{e}(j) = (29, 0, 0, 0, 0)$. Тогда получаем

$$r^1(j) = \hat{r}^1(j) - \overline{e}(j) = (25^*, 14, 13, 13, 25) - (29, 0, 0, 0, 0) = (27, 14, 13, 13, 25).$$

Ошибка исправлена.

Представленный в статье алгоритм позволяет корректировать ошибки в коде, состоящем из остатков по одному модулю. При этом для реализации приведенного примера кроме шести LUT-таблиц, реализующих вычисление ответа, потребуется дополнительно ввести 4 LUT-таблицы для вычисления двух контрольных остатков, две LUT-таблицы для вычисления синдрома ошибки и одну LUT-таблицу для хранения вектора ошибки. При использовании метода троированного резервирования потребуется 18 LUT-таблиц, реализующих вычисление ответа. Таким образом, разработанный алгоритм требует в 1,38 раза меньше схемных затрата, чем при использовании метода коррекции ошибок «2 из 3».

Выводы

В статье рассмотрен метод построения системы опознавания космического аппарата для низкоорбитальной группировки спутников, использующий полиномиальные модулярные коды. Показана актуальность коррекции искаженных ответов на вопросы запросчика, которые могут возникнуть из-за отказа оборудования ответчика, расположенного на борту. Для решения данной задачи был разработан алгоритм коррекции ошибок на основе свертки информационных остатков. Представленный пример показал эффективность разработанного алгоритма для кода, в котором все остатки получены по одному модулю, по обнаружению и коррекции однократной ошибки. При этом разработанный алгоритм при использовании трех информационных оснований ПМК требует в 1,38 раза меньше схемных затрат чем метод коррекции ошибок «2 из 3».

Список литературы

1. Анпилогов В.Р. Эффективность низкоорбитальных систем спутниковой связи на основе малых космических аппаратов // Технологии и средства связи. 2015. № 4. С. 62–67.

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

3. Пашинцев В.П., Калмыков М.И., Вельц О.В. Методы защиты передаваемой информации для системы удаленного контроля и управления высокотехнологическими объектами // Вестник Северо-Кавказского федерального университета. 2014 . № 2. С. 30–35.

4. Pashintsev V.P., Kalmykov I.A., Zhuk A.P., Kalmykov M.I., 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. Vol. 9. Issue 5. P. 958–965.

5. Степанова Е.П., Чистоусов Н.К., Тынчеров К.Т. Метод построения системы аутентификации спутника для низкоорбитальной системы спутниковой связи на основе целочисленных алгебраических структур полей Галуа // Современные наукоемкие технологии. 2019. № 7. С. 35–40.

6. Kalmykov I.A., Pashintsev V.P., Zhuk A.P., Chistousov N.K., Olenev A.A. 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. 2019. Vol. 8. Issue5. P. 2557–2562.

7. Omondi A., Premkumar B. Residue Number Systems: Theory and Implementation. Imperial College Press. UK, 2016. 293 p.

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