УДК 004.052:629.78

МЕТОД ПОСТРОЕНИЯ СИСТЕМЫ АУТЕНТИФИКАЦИИ СПУТНИКА ДЛЯ НИЗКООРБИТАЛЬНОЙ СИСТЕМЫ СПУТНИКОВОЙ СВЯЗИ НА ОСНОВЕ ЦЕЛОЧИСЛЕННЫХ АЛГЕБРАИЧЕСКИХ СТРУКТУР ПОЛЕЙ ГАЛУА

[1]Калмыков И.А., [1]Степанова Е.П., [1]Чистоусов Н.К., [1]Калмыков М.И., [2]Тынчеров К.Т.

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

[2]ФГБОУ ВО «Уфимский государственный нефтяной технический университет», филиал, Октябрьский

Перспективным направлением применения низкоорбитальных систем спутниковой связи являются автоматизированные системы дистанционного мониторинга, контроля и управления объектами добычи и транспортировки углеводородов Крайнего Севера. Для организации бесперебойной связи необходимо в состав группировки включить до 60 спутников. По мере увеличения числа стран, осваивающих месторождения Арктического шельфа, будет возрастать и количество группировок космических аппаратов. Это может привести к ситуации, когда спутник-нарушитель, оказавшись в зоне радиовидимости приемника, который располагается на абонентском терминале объекта, может навязать ранее перехваченную команду управления. В результате этого необслуживаемый объект добычи и транспортировки углеводородов может выйти из строя. Для предотвращения такой ситуации в статье предлагается использовать систему опознавания «свой-чужой». Для обеспечения высокой информационной скрытности в таких системах целесообразно использовать протокол аутентификации с нулевым разглашением знаний. С целью повышения скорости опознавания спутника предлагается использовать метод построения системы аутентификации КА низкоорбитальной системы спутниковой связи, использующий целочисленные алгебраические структуры конечных полей Галуа. Особое место среди последних занимают полиномиальные модулярные коды (ПМК), в которых арифметические операции выполняются независимо и параллельно по основаниям – неприводимым полиномам. Целью статьи является сокращение времени аутентификации спутника за счет использования ПМК.

Ключевые слова: система аутентификации космического аппарата, модулярные коды, метод построения системы аутентификации, полиномиальные модулярные коды

THE METHOD OF CONSTRUCTING THE AUTHENTICATION SYSTEM OF THE SATELLITE FOR A LEO SATELLITE COMMUNICATION SYSTEM ON THE BASIS OF INTEGER ALGEBRAIC STRUCTURES OF GALOIS FIELDS

[1]Kalmykov I.A., [1]Stepanova E.P., [1]Chistousov N.K., [1]Kalmykov M.I., [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

Automated systems for remote monitoring, control and management of hydrocarbon production and transportation facilities in the Far North are a promising area of application of low-orbit satellite communication systems. For the organization of uninterrupted communication it is necessary to include up to 60 satellites in the group. As the number of countries developing Arctic shelf deposits increases, the number of spacecraft groupings will also increase. This can lead to a situation where the intruder satellite, being in the radio visibility zone of the receiver, which is located on the subscriber terminal of an unattended object, can impose a previously intercepted control command. As a result, the maintenance-free hydrocarbon production and transportation facility may fail. To prevent this situation, the article proposes to use the system of identification «friend or foe». To ensure high information secrecy in such systems, it is advisable to use the authentication Protocol with zero-knowledge proof knowledge. In order to increase the speed of identification of satellite b, it is proposed to use the method of constructing an authentication system for spacecraft of low-orbit satellite communication system using integer algebraic structures of finite Galois fields. A special place among the latter is occupied by polynomial modular codes (PMC), in which arithmetic operations of codes are performed independently and in parallel on bases – irreducible polynomials. The aim of the article is to reduce the time of satellite authentication by using polynomial modular codes.

Keywords: authentication system of the spacecraft, modular codes, the method of constructing the authentication system, polynomial modular codes

Известно, что низкоорбитальные системы спутниковой связи нашли широкое применение в таких глобальных проектах, как освоение Северного морского пути, создание информационно-телеметрических систем воздушного и наземного транспорта в высоких широтах. Особое место занимают проекты освоения шельфа Северного Ледовитого океана. В этом НССС входят в состав автоматизированных систем дистанционного мониторинга, контроля и управления (АСДМКУ) объектами добычи и транспортировки углеводородов [1]. Для организации связи состав группировки содержит от 48 до 60 спутников. Увеличение количества НССС может привести к ситуации, когда спутник-

нарушитель попытается навязать перехваченную и задержанную команду управления, что приведет к отказу объекта управления.

Устранить такую ситуацию можно за счет повышения информационной скрытности НССС с помощью системы аутентификации спутника (САС) [2]. Чтобы повысить скорость аутентификации спутника, необходимо перейти к параллельным вычислениям, то есть использовать целочисленные алгебраические структуры полей Галуа – полиномиальные модулярные коды (ПМК). Применение данных кодов позволяет осуществить распараллелить вычисления на уровне арифметических операций. Поэтому разработка метода построения САС, базирующейся на ПМК**,** является актуальной задачей.

Материалы и методы исследования

Очевидно, что эффективность обеспечения информационной скрытности НССС определяется протоколом аутентификации, который используется в системе аутентификации спутника. Проведенный анализ работ [3, 4] показал, что множество протоколов аутентификации можно разбить на три группы. В первую группу входят протоколы парольной аутентификации. Однако данные протоколы аутентификации не могут использоваться для опознавания спутника, так как имеют низкую криптографическую стойкость. Основу второй группы составляют протоколы аутентификации типа «запрос – ответ». В этих протоколах, согласно [4], широко используются алгоритмы шифрования. Однако данные протоколы нельзя использовать в САС, так как необходимо хранить секретные ключи не только на спутниках и объектах.

Этого недостатка лишены протоколы аутентификации с нулевым разглашением знаний, которые образуют третью группу. Однако в таких протоколах необходимо выполнить от 40 раундов идентификации [4]. Снизить временные затраты позволяет протокол, который представлен в работе [5]. Он состоит из следующих этапов.

Для работы САС выбирают большое простое число M, а также секретный ключ K, параметры S и T, удовлетворяющие $\{K,S,T\} < M-1$. С помощью S и T вычисляются сеансовые ключи и параметр проверки повторного их использования

$$S(j) = g^{\left(\prod_{i=1}^{n}(S_i\,(j-1)+K_i)\right)^{-1}} \bmod M,$$

$$T(j) = g^{\left(\prod_{i=1}^{n}(S_i\,(j-1)+K_i+T_i)\right)^{-1}} \bmod M, \qquad (1)$$

где $\{K_i, S_i, T_i\}$ – i-е блоки секретного ключа K, S и T; g – порождающий элемент; $\lceil \log_2 M \rceil = m_i n$; n – количество блоков размерностью m_i разрядов каждый.

Первый этап. Перед началом j-го сеанса работы САС определяется истинный статус спутника, используя сеансовый ключ $S(j)$ и параметры и параметр $T(j)$, согласно

$$C(j) = g^K g^{S(j)} g^{T(j)} \bmod M. \qquad (2)$$

Второй этап. Производится вычисление зашумленного статуса спутника, используя зашумленные значения K, $S(j)$ и T(j), согласно

$$C^*(j) = g^{K^*(j)} g^{S^*(j)} g^{T^*(j)} \bmod M, \qquad (3)$$

где $\{\Delta K(j), \Delta S(j), \Delta T(j)\} \le M-2$ – случайные числа зашумления; $K^*(j) = |K + \Delta K(j)|^+_{\varphi(M)}$; $S^*(j) = |S(j) + \Delta S(j)|^+_{\varphi(M)}$; $T^*(j) = |T(j) + \Delta T(j)|^+_{\varphi(M)}$.

Процедура аутентификации статуса спутника включает следующих два этапа.

Первый этап. Запросчик генерирует число $d(j) < M-2$, которое называется запросом, а затем передает его ответчику КА.

Второй этап. Ответчик отвечает на запрос $d(j)$ согласно

$$r_1(j) = |K^*(j) - d(j)K(j)|^+_{\varphi(M)},$$

$$r_2(j) = |S^*(j) - d(j)S(j)|^+_{\varphi(M)},$$

$$r_3(j) = |T^*(j) - d(j)T(j)|^+_{\varphi(M)}, \qquad (4)$$

где $\varphi(M)$ – функция Эйлера простого числа M.

Затем ответчик пересылает запросчику сигнал в виде $\{C(j), C^*(j), r_1(j)\, r_2(j)\, r_3(j)\}$.

Процесс аутентификации спутника реализуется с помощью выражения

$$Y(j) = (C(j))^{d(j)} g^{r_1(j)} g^{r_2(j)} g^{r_3(j)} \bmod M. \qquad (5)$$

Если результат совпал с $C^*(j)$, то спутник является «своим», и он может начать сеанс связи. В противном случае – спутник к каналу связи не допускается.

Согласно [4] для обеспечения высокой имитостойкости протокола аутентификации необходимо чтобы M имело не менее 128 разрядов, что приводит к значительным временным затратам на реализацию мультипликативных операций. Снизить время опознавания КА можно за счет использования целочисленных алгебраических структур полей Галуа, то есть ПМК.

В этих кодах в качестве оснований используются неприводимые полиномы $p_i(x)$, где $i = 1, 2,..., k$. Тогда целое число F переводится в полиномиальную форму $F(x)$, которая заменяется набором остатков $F(x) = (F_1(x), F_2(x),..., F_k(x))$, где $F_i(x) \equiv F(x) \bmod p_i(x)$ [6]. Тогда для полиномиальных модулярных кодов справедливы выражения

$$F(x) \oplus G(x) = ((F_1(x) \oplus G_1(x)) \bmod p_1(x), ..., (F_k(x) \oplus G_k(x)) \bmod p_k(x)), \qquad (6)$$

$$F(x) \cdot G(x) = ((F_1(x) \cdot G_1(x)) \bmod p_1(x), ..., (F_k(x) \cdot G_k(x)) \bmod p_k(x)), \qquad (7)$$

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

Кортеж оснований ПМК задает величину рабочего диапазона

$$P(x) = \prod_{i=1}^{k} p_i(x). \quad (8)$$

Реализуем одномодульный протокол аутентификации спутника [5] с использованием целочисленных алгебраических структур полей Галуа. Выбираем параметры протокола, удовлетворяющие условию $\log_2\{K, S(j), T(j)\} < \deg P(x)$, где $\deg P(x)$ – степень полинома $P(x)$. Проводим конкатенацию выбранных параметров $K = (K_1 \| K_2 \| ... \| K_k)$, $S^j = (S_1^j \| S_2^j \| ... \| S_k^j)$ и $T^j = (T_1^j \| T_2^j \| ... \| T_k^j)$, где $K_i = \deg p_i(x)$, $S_i^j = \deg p_i(x)$; $T_i^j = \deg p_i(x)$; $i = 1, 2,..., k$. Пусть порождающий элемент $g = x$.

Рассмотрим выполнение предварительных вычислений на j-ом сеансе проверки:

Первый этап. Ответчик, располагаемый на КА, определяет истинный статус

$$C^j(x) = \left(\left| g(x)^{K_1} g(x)^{S_1^j} g(x)^{T_1^j} \right|^{+}_{p_i(x)}, ..., \left| g(x)^{K_k} g(x)^{S_k^j} g(x)^{T_k^j} \right|^{+}_{p_i(x)} \right). \quad (9)$$

Второй этап. Ответчик для вычисления зашумленного статуса КА выбирает случайные числа $\left\{\Delta K_i, \Delta S_i^j, \Delta T_i^j\right\} < 2^{\deg p_i(x)} - 1$ и производит вычисление параметров

$$\tilde{K}_i^j = \left| K_i + \Delta K_i^j \right|^{+}_{2^{\deg p_i(x)}-1}, \quad \tilde{S}_i^j = \left| S_i^j + \Delta S_i^j \right|^{+}_{2^{\deg p_i(x)}-1}, \quad \tilde{T}_i^j = \left| T_i^j + \Delta T_i^j \right|^{+}_{2^{\deg p_i(x)}-1}. \quad (10)$$

Ответчик определяет зашумленный статус спутника, используя ПМК

$$\tilde{C}^j(x) = \left(\left| g(x)^{\tilde{K}_1^j} g(x)^{\tilde{S}_1^j} g(x)^{\tilde{T}_1^j} \right|^{+}_{p_i(x)}, ..., \left| g(x)^{\tilde{K}_k} g(x)^{\tilde{S}_k^j} g(x)^{\tilde{T}_k^j} \right|^{+}_{p_i(x)} \right). \quad (11)$$

Процедура аутентификации статуса спутника.

Первый этап. Запросчик передает спутнику в качестве запроса случайное число $d^j = (d_1^j, d_2^j, ... d_k^j)$, где $d_i^j \equiv d^j \bmod 2_i^{\deg p_i(x)} - 1$; $i = 1, 2,..., k$.

Второй этап. Ответчик получает ответы на запрос $d^j = (d_1^j, d_2^j, ... d_k^j)$, согласно

$$r_i^1(j) = \left| \tilde{K}_i^j + d_i^j K_i^j \right|^{+}_{2^{\deg p_i(x)}-1}, \quad r_i^2(j) = \left| \tilde{S}_i^j + d_i^j S_i^j \right|^{+}_{2^{\deg p_i(x)}-1}, \quad r_i^3(j) = \left| \tilde{T}_i^j + d_i^j T_i^j \right|^{+}_{2^{\deg p_i(x)}-1}. \quad (12)$$

Спутник передает запросчику следующие данные

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

Процедура проверки ответов.

1. Запросчик проверяет ответы на вопрос $d^j = (d_1^j, d_2^j, ... d_k^j)$.

$$Y_i^j(x) = \left| \left(C_i^j(x) \right)^{d_i^j} g(x)^{r_i^1} g(x)^{r_i^2} g(x)^{r_i^3} \right|^{+}_{p_i(x)}. \quad (13)$$

Спутнику присвоят статус «свой», если справедливо

$$\left\{ Y_1^j(x) = \tilde{C}_1^j(x), Y_2^j(x) = \tilde{C}_2^j(x), ..., Y_k^j(x) = \tilde{C}_k^j(x) \right\}. \quad (14)$$

Результаты исследования и их обсуждение

В качестве оснований $p_1(x) = x^5 + x^3 + x^2 + x + 1$, $p_2(x) = x^5 + x^4 + x^2 + x + 1$, $p_3(x) = x^5 + x^4 + x^3 + x + 1$, $p_4(x) = x^5 + x^4 + x^3 + x^2 + 1$. Значит, размер секретного ключа K, параметров S и T не должны превышать 20 разрядов. Пусть $K = 836931$, $S = 467430$ и $T = 108667$. В табл. 1 представлена их конкатенация.

Таблица 1

Двоичный код и конкатенация параметров протокола

Параметры	Двоичный код и конкатенация																			
$K = 836931$	1	1	0	0	1	1	0	0	0	1	0	1	0	1	0	0	0	0	1	1
$K_1 \parallel K_2 \parallel K_3 \parallel K_4$	25_{10}					17_{10}					10_{10}					3_{10}				
$S = 467430$	0	1	1	1	0	0	1	0	0	0	0	1	1	1	1	0	0	1	1	0
$S_1^j \parallel S_2^j \parallel S_3^j \parallel S_4^j$	14_{10}					8_{10}					15_{10}					6_{10}				
$T = 108667$	0	0	0	1	1	0	1	0	1	0	0	0	0	1	1	1	1	0	1	1
$T_1^j \parallel T_2^j \parallel T_3^j \parallel T_4^j$	3_{10}					10_{10}					3_{10}					27_{10}				

1. Ответчик вычисляет истинный статус, представленный в ПМК, используя (9):

$$C_1^j(x) = \left| g(x)^{K_1}\, g(x)^{S_1^j}\, g(x)^{T_1^j} \right|^+_{p_i(x)} = \left| x^{25} \cdot x^{14} \cdot x^3 \right|^+_{p_1(x)} = \left| x^{11} \right|^+_{p_1(x)} = x^4 + x^2 + x,$$

$$C_2^j(x) = \left| g(x)^{K_2}\, g(x)^{S_2^j}\, g(x)^{T_2^j} \right|^+_{p_2(x)} = \left| x^{17} \cdot x^8 \cdot x^{10} \right|^+_{p_2(x)} = \left| x^4 \right|_{p_2(x)} = x^4,$$

$$C_3^j(x) = \left| g(x)^{K_3}\, g(x)^{S_3^j}\, g(x)^{T_3^j} \right|^+_{p_i(x)} = \left| x^{10} \cdot x^{15} \cdot x^3 \right|^+_{p_3(x)} = \left| x^{28} \right|^+_{p_3(x)} = x^4 + x^2,$$

$$C_4^j(x) = \left| g(x)^{K_4}\, g(x)^{S_4^j}\, g(x)^{T_4^j} \right|^+_{p_4(x)} = \left| x^3 \cdot x^6 \cdot x^{27} \right|^+_{p_3(x)} = \left| x^5 \right|^+_{p_4(x)} = x^4 + x^3 + x^2 + 1.$$

2. Ответчик для вычисления зашумленного статуса КА выбирает случайные числа $\left\{\Delta K_i, \Delta S_i^j, \Delta T_i^j\right\} < 2^5 - 1$. Результаты зашумления согласно (10) приведены в табл. 2.

Таблица 2

Зашумление параметров протокола

Параметры	Зашумленные значения параметров K, *S*, T			
$K_1 \parallel K_2 \parallel K_3 \parallel K_4$	25_{10}	17_{10}	10_{10}	3_{10}
ΔK_i^j	2_{10}	5_{10}	3_{10}	4_{10}
$\tilde{K}_1 \parallel \tilde{K}_2 \parallel \tilde{K}_3 \parallel \tilde{K}_4$	27_{10}	22_{10}	13_{10}	7_{10}
$S_1^j \parallel S_2^j \parallel S_3^j \parallel S_4^j$	14_{10}	8_{10}	15_{10}	6_{10}
ΔS_i^j	10_{10}	4_{10}	8_{10}	24_{10}
$\tilde{S}_1^j \parallel \tilde{S}_2^j \parallel \tilde{S}_3^j \parallel \tilde{S}_4^j$	24_{10}	12_{10}	23_{10}	30_{10}
$T_1^j \parallel T_2^j \parallel T_3^j \parallel T_4^j$	3_{10}	10_{10}	3_{10}	27_{10}
ΔT_i^j	11_{10}	9_{10}	26_{10}	2_{10}
$\tilde{T}_1^j \parallel \tilde{T}_2^j \parallel \tilde{T}_3^j \parallel \tilde{T}_4^j$	14_{10}	19_{10}	29_{10}	29_{10}

Согласно (11) ответчик определяет зашумленный статус спутника, используя ПМК

$$\tilde{C}_1^j(x) = \left| g(x)^{\tilde{K}_1}\, g(x)^{\tilde{S}_1^j}\, g(x)^{\tilde{T}_1^j} \right|^+_{p_i(x)} = \left| x^{27} \cdot x^{24} \cdot x^{14} \right|^+_{p_1(x)} = \left| x^3 \right|_{p_1(x)} = x^3,$$

$$\tilde{C}_2^j(x)=\left|g(x)^{\tilde{K}_2^j}\,g(x)^{\tilde{S}_2^j}\,g(x)^{\tilde{T}_2^j}\right|^+_{p_2(x)}=\left|x^{22}\cdot x^{12}\cdot x^{19}\right|^+_{p_2(x)}=\left|x^{22}\right|_{p_2(x)}=x^4+x^3,$$

$$\tilde{C}_3^j(x)=\left|g(x)^{\tilde{K}_3^j}\,g(x)^{\tilde{S}_3^j}\,g(x)^{\tilde{T}_3^j}\right|^+_{p_i(x)}=\left|x^{13}\cdot x^{23}\cdot x^{29}\right|^+_{p_3(x)}=\left|x^{3}\right|_{p_3(x)}=x^3,$$

$$\tilde{C}_4^j(x)=\left|g(x)^{\tilde{K}_4^j}\,g(x)^{\tilde{S}_4^j}\,g(x)^{\tilde{T}_4^j}\right|^+_{p_4(x)}=\left|x^{7}\cdot x^{30}\cdot x^{29}\right|^+_{p_4(x)}=\left|x^{4}\right|_{p_4(x)}=x^4.$$

Рассмотрим процесс аутентификации статуса спутника.

1. Запросчик передает спутнику в качестве запроса случайное число $d^j=(d_1^j,d_2^j,d_3^j,d_4^j)=(4,4,4,4)$.

2. Ответчик вычисляет ответы на запрос, согласно выражения (12). Тогда ответы по первому модулю будут равны

$$r_1^1(j)=\left|\tilde{K}_1^j-d_1^j\cdot K_1\right|^+_{31}=\left|27-4\cdot 25\right|^+_{31}=20,\;\; r_1^2(j)=\left|\tilde{S}_1^j-d_1^j\cdot S_1^j\right|^+_{31}=\left|24-4\cdot 14\right|^+_{31}=\left|-1\right|^+_{31}=30,$$
$$r_1^3(j)=\left|\tilde{T}_1^j-d_1^j\cdot T_1^j\right|^+_{31}=\left|14-4\cdot 3\right|^+_{31}=\left|2\right|^+_{31}=2.$$

Ответы по второму модулю будут равны

$$r_2^1(j)=\left|\tilde{K}_2-d_2^j\cdot K_2\right|^+_{31}=\left|22-4\cdot 17\right|^+_{31}=16,\;\; r_2^2(j)=\left|\tilde{S}_2^j-d_2^j\cdot S_2^j\right|^+_{31}=\left|12-4\cdot 8\right|^+_{31}=11,$$
$$r_2^3(j)=\left|\tilde{T}_2^j-d_2^j\cdot T_2^j\right|^+_{31}=\left|19-4\cdot 10\right|^+_{31}=\left|-21\right|^+_{31}=\left|31-21\right|^+_{31}=10.$$

Ответы по третьему модулю будут равны

$$r_3^1(j)=\left|\tilde{K}_3^j-d_3^j\cdot K_3\right|^+_{31}=\left|13-4\cdot 10\right|^+_{31}=4,\;\; r_3^2(j)=\left|\tilde{S}_3^j-d_3^j\cdot S_3^j\right|^+_{31}=\left|23-4\cdot 15\right|^+_{31}=25,$$
$$r_3^3(j)=\left|\tilde{T}_3^j-d_3^j\cdot T_3^j\right|^+_{31}=\left|29-4\cdot 3\right|^+_{31}=\left|17\right|^+_{31}=17.$$

Ответы по четвертому модулю будут равны

$$r_4^1(j)=\left|\tilde{K}_4^j-d_4^j\cdot K_4\right|^+_{31}=\left|7-4\cdot 3\right|^+_{31}=26,\;\; r_4^2(j)=\left|\tilde{S}_4^j-d_4^j\cdot S_4^j\right|^+_{31}=\left|30-4\cdot 6\right|^+_{31}=\left|6\right|^+_{31}=6,$$
$$r_4^3(j)=\left|\tilde{T}_4^j-d_4^j\cdot T_4^j\right|^+_{31}=\left|29-4\cdot 27\right|^+_{31}=\left|-17\right|^+_{31}=\left|31-17\right|^+_{31}=14.$$

Спутник передает запросчику следующие данные:

– истинные статусы $\left\{C_1^j(x),C_2^j(x),C_3^j(x),C_4^j(x)\right\}=\left\{10110,10000,10100,11101\right\}$;

– зашумленные статусы $\left\{\tilde{C}_1^j(x),\tilde{C}_2^j(x),\tilde{C}_3^j(x),\tilde{C}_4^j(x)\right\}=\left\{01000,11000,01000,10000\right\}$;

– первая группа ответов $\left\{r_1^1(j),r_1^2(j),r_1^3(j)\right\}=\left\{10100,11110,00010\right\}$;

– вторая группа ответов $\left\{r_2^1(j),r_2^2(j),r_2^3(j)\right\}=\left\{10000,01011,01010\right\}$;

– третья группа ответов $\left\{r_3^1(j),r_3^2(j),r_3^3(j)\right\}=\left\{00100,11001,10001\right\}$;

– четвертая группа ответов $\left\{r_4^1(j),r_4^2(j),r_4^3(j)\right\}=\left\{11010,00110,01110\right\}$.

Рассмотрим процедуру проверки ответов согласно выражению (13). Получаем

$$Y_1^j(x)=\left|\left(C_1^j(x)\right)^{d_1^j}\,g(x)^{r_1^1}\,g(x)^{r_1^2}\,g(x)^{r_1^3}\right|^+_{p_1(x)}=\left|\left(x^4+x^2+x\right)^4\cdot x^{20}\cdot x^{30}\cdot x^2\right|^+_{p_1(x)}=x^3,$$

$$Y_2^j(x)=\left|\left(C_2^j(x)\right)^{d_2^j}\,g(x)^{r_2^1}\,g(x)^{r_2^2}\,g(x)^{r_2^3}\right|^+_{p_2(x)}=\left|\left(x^4\right)^4\cdot x^{16}\cdot x^{11}\cdot x^{10}\right|^+_{p_2(x)}=x^4+x^3,$$

$$Y_3^j(x)=\left|\left(C_3^j(x)\right)^{d_3^j} g(x)^{r_3^1} g(x)^{r_3^2} g(x)^{r_3^3}\right|^{+}_{p_3(x)}=\left|\left(x^4+x^2\right)^4\cdot x^4\cdot x^{25}\cdot x^{17}\right|^{+}_{p_3(x)}=x^3,$$

$$Y_4^j(x)=\left|\left(C_4^j(x)\right)^{d_4^j} g(x)^{r_4^1} g(x)^{r_4^2} g(x)^{r_4^3}\right|^{+}_{p_4(x)}=\left|\left(x^4+x^3+x^2+1\right)^4\cdot x^{26}\cdot x^6\cdot x^{14}\right|^{+}_{p_4(x)}=x^4.$$

Полученные значения совпали с зашумленным статусом КА, представленным в ПМК. Значит, статус аутентифицируется как «свой», и ему предоставляется сеанс связи.

В рассмотренном примере использование разработанного метода построения САС на основе ПМК позволило повысить скорость аутентификации спутника. Известно, что время выполнения мультипликативных операций пропорционально разряду операндов. При использовании одномодульного протокола аутентификации разрядность данных составляла 20 разрядов. При переходе к ПМК разрядность операндов сократилась до 5 бит. Значит, за счет распараллеливания вычислений на уровне операций в ПМК скорость аутентификации КА повысилась в 4 раза по сравнению с протоколом [5].

Выводы

В статье представлен разработанный метод построения системы аутентификации спутника для НССС на основе полиномиальных модулярных кодов. Распараллеливание вычислений на уровне операций, которое обеспечивают ПМК, повысит скорость аутентификации спутника. В приведенном в статье примере был использован протокол аутентификации, в котором разрядность данных составляла 20 разрядов. При переходе к ПМК разрядность операндов сократилась до 5 бит. Значит, за счет распараллеливания вычислений на уровне операций в ПМК скорость аутентификации КА повысилась в 4 раза по сравнению с протоколом [4].

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

Список литературы

1. Алёшин Б.С., Баженов С.Г., Диденко Ю.И. Системы дистанционного управления. М.: Изд-во «Наука», 2013. 292 с.

2. 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. P. 958–965.

3. Smith R. Authenticaton: From Passwords to Public Keys. New York: Addison-Wesley Publishing Company, Inc., 2015. 352 p.

4. Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности. М.: Горячая линия-Телеком, 2011. 256 с.

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

6. Stepanova E.P., Toporkova E.V., Katkov R.A., Rezenkov D.N. Application of the codes of a polynomial residue number system, aimed at reducing the effects of failures in the AES cipher. Journal of Digital Information Management. 2016. № 14 (2). P 114–123.