Разработка методики построения отказоустойчивой системы аутентификации низкоорбитальных спутников, функционирующей в полиномиальной системе классов вычетов

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

Северо-Кавказский федеральный университет, Ставрополь, Россия

Аннотация: Одним из эффективных способов повышения информационной скрытности группировки низкоорбитальных космических аппаратов (НКА) является применение системы аутентификации спутника (САС). С целью снижения временных затрат на определение статуса НКА, а также повышения отказоустойчивости системы опознавания в ряде работ предлагается использовать коды полиномиальной системы классов вычетов (ПСКВ). В данной работе представлена методика построения отказоустойчивой системы аутентификации космического аппарата, которая построена на обменных операциях, реализуемых в кодах ПСКВ. Используя обменные операции, то есть, изменяя количество информационных и избыточных оснований, можно обеспечить возможность сохранения работоспособного состояния системы опознавания при возникновении последовательности отказов, в результате чего уровень информационной скрытности НКА не будет снижен.
Ключевые слова: система аутентификации спутника, полиномиальная система классов вычетов, обменные операции, методика построения отказоустойчивой системы опознавания.

Введение

В настоящее время успешная реализация проектов, направленных на развитие районов Крайнего Севера, невозможна без использования группировок низкоорбитальных космических аппаратов (далее НКА). Для обеспечения надежной и высокоскоростной передачи данных предлагается увеличивать как число спутников, так и количество их группировок. Так в ответственном проекте «Сфера» предлагается применение 640 спутников [1] Такое большое число НКА позволит реализовать в реальном масштабе времени не только телефонную и интернет-связь, но и решить вопросы мониторинга транспорта [2]. Однако, рост числа группировок НКА, в том числе и иностранных, может спровоцировать навязывание «чужого» контента абонентам.

Для предотвращения данной ситуации предлагается повышать информационную скрытность низкоорбитальной группировки космических

аппаратов за счет использования системы аутентификации спутника (далее САС), функционирующей в полиномиальной системе классов вычетов (далее ПСКВ) [3]. Применение кодов ПСКВ способствует снижению временных затрат на определение статуса НКА, а также повышению отказоустойчивости системы опознавания за счет коррекции ошибок, возникающих при выполнении протокола аутентификации. Повысить отказоустойчивость САС возможно за счет использования обменных операций ПСКВ, которые позволяют изменять количество информационных и избыточных оснований при возникновении отказов вычислительных трактов модулярного кода. Благодаря этому сохраняется работоспособное состояние системы опознавания при возникновении последовательности отказов, в результате чего уровень информационной скрытности НКА не будет снижен. Поэтому разработка методики построения отказоустойчивой САС, функционирующей в полиномиальной системе классов вычетов, является актуальной задачей.

Цель исследования

Для предотвращения навязывания «чужого» контента с помощью НКА применяются САС, использующие протоколы аутентификации с нулевым разглашением сведений, реализованные в ПСКВ. Независимая и параллельная организация вычислений в ПСКВ позволяет не только снизить временные затраты на опознавание спутника, но и повысить его отказоустойчивость за счет коррекции ошибок, возникающих в процессе реализации протокола аутентификации [4]. Дальнейшее повышение отказоустойчивости САС возможно за счет использования методики построения отказоустойчивой САС, функционирующей в ПСКВ. Цель работы – повышение отказоустойчивости системы аутентификации низкоорбитальных спутников за счет применения разработанной методики построения отказоустойчивой САС на основе обменных операций кода ПСКВ.

Материалы и методы

Математической основой кода ПСКВ является набор неприводимых полиномов $p_i(x)$, где $i=1,2,\ldots,k$, который задает предельную разрядность рабочего диапазона [5,6]

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

Тогда, используя выражение (1) и условие $\deg M(x)<\deg P_k(x)$, можно полином $M(x)$ представить в коде ПСКВ в виде

$$M(x)=(M_1(x),M_2(x),\ldots,M_k(x)), \quad (2)$$

где $M_i(x)\equiv M(x)\bmod p_i(x);\ i=1,2,\ldots,k$.

В кодах ПСКВ операции сложения, вычитания и умножения относятся к модульным операциям, для которых справедливо

$$\begin{aligned} M(x)\pm C(X)&=(M_1(x)\pm C_1(x)\bmod p_1(x),\ldots,M_k\pm C_k(x)\bmod p_k(x)),\\ M(x)\cdot C(X)&=(M_1(x)\cdot C_1(x)\bmod p_1(x),\ldots,M_k\cdot C_k(x)\bmod p_k(x)), \end{aligned} \quad (3)$$

где $C_i(x)\equiv C(x)\bmod p_i(x);\ \deg C(x)<\deg P_k(x);i=1,2,\ldots,k$.

Из выражения (3) видно, что остатки в коде ПСКВ складываются, вычитаются и умножаются помодульно, параллельно и независимо. Это позволяет не только повысить скорость вычислений, но и используется для построения корректирующих модулярных кодов. Согласно [5] введение r избыточных неприводимых полиномов увеличивает число оснований кода ПСКВ до $n=k+r$ и позволяет исправлять ошибки кратности $\lfloor r/2\rfloor$. В этом случае рабочий диапазон расширяется до полного:

$$P_n(x)=\prod_{i=1}^{n} p_i(x). \quad (4)$$

Тогда, учитывая равенство (4), выражение (2) кода ПСКВ примет вид:

$$M(x)=(M_1(x),M_2(x),\ldots,M_k(x),M_{k+1}(x),\ldots,M_n(x)), \quad (5)$$

где $M_i(x)\equiv M(x)\bmod p_i(x);\ \deg M(x)<\deg P_n(x);i=1,2,\ldots,n$.

При этом избыточные основания ПСКВ должны удовлетворять

$$\deg p_k(x) \le \deg p_{k\_1}(x) \le \deg p_{k+2}(x) \le \ldots \le + \deg p_n(x). \quad (6)$$

Согласно [5] комбинация кода ПСКВ, определяемая выражением (5), не содержит ошибок, если для нее справедливо:

$$\deg M(x) < \deg P_k(x). \quad (7)$$

В работах [5-9] представлены алгоритмы поиска и коррекции ошибок в коде ПСКВ, которые возникают из-за сбоев и отказов вычислительных трактов в процессе выполнения протокола аутентификации. Однако в данных работах не были рассмотрены вопросы использования обменных операций для повышения отказоустойчивости САС.

Согласно [5] обменные операции позволяют изменять точность, производительность и информационную достоверность проводимых вычислений за счет изменения соотношений между числом информационных и избыточных оснований в кортеже кода ПСКВ. Это связано с тем, что информационные и проверочные остатки кода ПСКВ зависят только от исходного полинома M(x).

Положим, что для обеспечения требуемой точности вычислений достаточно $k-2$ информационных оснований. Это приведет к уменьшению рабочего диапазона кода, так как, согласно выражению (1), он будет равен:

$$\deg P_{k-2}(x) = \prod_{i=1}^{k-2} p_i(x) < \deg P_k(x). \quad (8)$$

Анализ выражения (8) показывает, что в этом случае уменьшается точность проводимых вычислений. Однако при этом увеличилось число избыточных неприводимых оснований, так как, $r_{k-2} = n - (k-2) = r_k + 2$. В этом случае за счет обменных операций код ПСКВ сможет исправлять ошибки более высокой кратности $\lfloor r_{k-2}/2 \rfloor = \lfloor r_k/2 \rfloor + 1$. При этом уменьшение числа информационных оснований позволяет повысить производительность вычислений, так как временные затраты на выполнение обязательной

немодульной операции обратного преобразования из ПСКВ в позиционную систему счисления пропорционально числу информационных оснований модулярного кода [5].

На рис.1 показано влияние обменных операций кода ПСКВ между информационными (k) и избыточными (r) основаниями на точность (H_1), информационную достоверность (H_2) и производительность (H_3) выполнения протокола аутентификации при условии, что $k + r = const$.

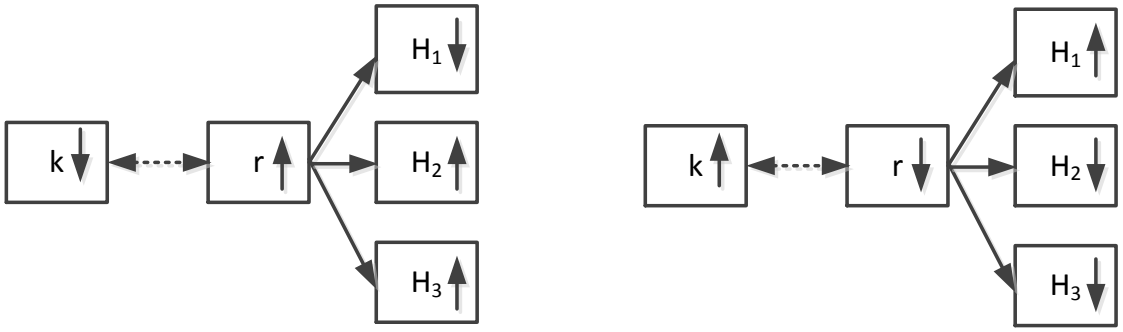

Рис 1. – Структура обменных операций ПСКВ

Таким образом, очевидно, что коды ПСКВ имеют потенциальную возможность в режиме вычислений динамически изменять такие показатели, как точность, информационную достоверность и производительность. Значит, используя обменные операции, можно парировать несколько отказов, возникающих друг за другом, за счет постепенного снижения основных показателей качества функционирования в допустимых пределах. Это сохранит работоспособное состояние вычислительной системы ПСКВ.

Наиболее сложной вычислительной процедурой при реализации вычислительной системы ПСКВ с реконфигурируемой структурой является пересчет значений ортогональных базисов при отказе оснований ПСКВ. В работе [10] представлен разработанный метод вычисления динамически изменяемого кортежа ортогональных базисов, позволяющего повысить отказоустойчивость системы опознавания спутника при ее реконфигурации.

Рассмотренные выше результаты положены в основу разработанной методики построения отказоустойчивой САС, функционирующей в ПСКВ. В качестве главной цели методики выбрано достижение максимальной отказоустойчивости системы аутентификации спутника при возникновении нескольких отказов, возникающих друг за другом, за счет постепенного снижения основных показателей качества функционирования в допустимых пределах. Для этого необходимо выполнить следующие этапы:

1 этап. Решается задача выбора протокола аутентификации с нулевым разглашением сведений w_e из множества $W=\{w_1, w_2, \ldots, w_E\}$ известных, поддерживающего параллельно-конвейерную организацию вычислений в кодах ПСКВ

$$\forall w_e \in W=\{w_1, w_2, \ldots, w_E\} \exists\, w_{опт} \in W\left[w_e = w_{опт} \rightarrow P(w_e) \leftrightarrow P(D)\right]. \qquad (9)$$

где $P(w_e)$ – алгоритм выполнения протокола аутентификации; $P(D)$ – параллельно-конвейерная организация вычислений в кодах ПСКВ.

2 этап. Решается задача выбора кортежа неприводимых полиномов для кода ПСКВ. Так как система аутентификации размещается на борту спутника, то при определении оснований ПСКВ надо обеспечить минимальные схемные затраты $V_{ПСКВ}$. При этом должна быть достигнута требуемая разрядность запросных и ответных слов. Тогда получаем:

$$\begin{cases} V_{ПСКВ}(\{p_i(x)\}) \rightarrow \min \\ Q_{ПСКВ}(\{p_i(x)\}) \geq Q_{доп} \end{cases}, \qquad (10)$$

где $Q_{ПСКВ}$ – рабочий диапазон кода ПСКВ, вычисленный согласно выражению (1) и определяемый разрядностью запросных и ответных слов; $Q_{доп}$ – допустимое значение разрядности запросных и ответных слов.

Для обеспечения свойства отказоустойчивости необходимо ввести избыточные основания ПСКВ, которые должны удовлетворять условию (6).

При этом необходимо учитывать кратность исправленных отказов $N_{ПСКВ}$. Тогда имеем:

$$\begin{cases} V_{ПСКВ}\left(\left\{p^k(x), p^r(x)\right\}\right) \to \min \\ N_{ПСКВ}\left(\left\{p^k(x), p^r(x)\right\}\right) \geq N_{доп} \end{cases}, \quad (11)$$

где $\left\{p_i^k(x)\right\}$ и $\left\{p_i^r(x)\right\}$ – кортежи информационных и избыточных оснований; $N_{доп}$ – предельно допустимое значение кратности исправленных отказов.

3 этап. Решается задача выбора алгоритма поиска и коррекции ошибок в кодах ПСКВ из условия:

$$\begin{cases} V_{\Sigma}\left(\left\{p^k(x), p^r(x)\right\}, u_j, f_d\right) \to \min \\ T_{кор}\left(\left\{p^k(x), p^r(x)\right\}, u_j\right) \leq T_{ПСКВ-ПСС}\left(\left\{p^k(x), p^r(x)\right\}, u_j\right), \\ N_{ПСКВ}\left(\left\{p^k(x), p^r(x)\right\}, u_j, f_d\right) \geq N_{доп} \end{cases} \quad (12)$$

где $V_{\Sigma} = V_{ПСКВ-ПСС} + V_{кор}$ – суммарные аппаратурные затраты на процедуры поиска и исправления ошибок и декодирования из кода ПСКВ в позиционный код; $N_{доп}$ – предельно допустимое число исправленных отказов, в процессе работы системы ПСКВ; $f_d \in F = [f_1, f_2, ..., f_M]$ - множество методов и алгоритмов вычисления позиционных характеристик (далее ПХ), применяемых для поиска и исправления ошибок в ПСКВ; $N_{ПСКВ}\left(\left\{p^k(x), p^r(x)\right\}, u_j, f_d\right)$ – число исправленных ошибок, вызванных отказами в процессе вычислений с помощью f_d алгоритма вычисления ПХ.

4 этап. Решается задача выбора соответствующего метода реконфигурации, базирующегося на обменных операциях кода ПСКВ. В результате будет обеспечено работоспособное состояние системы аутентификации спутника за счет постепенной деградации его структуры в заданных пределах. Для оценки эффективности предложенных решений выбираем критерий - коэффициент запаса работоспособности отказоустойчивого вычислительного устройства [11]

$$\delta_h = \frac{M_h}{G_h}, \qquad (13)$$

где M_h – количество работоспособных состояний системы аутентификации спутника при возникновении $h = 1, 2, \ldots$ отказов элементов; G_h – общее количество возможных состояний САС.

Тогда имеем следующую постановку задачи этапа:

$$\begin{cases} \sigma_h\left(\{p^k(z), p^r(z)\}, u_j, f_d, o_b\right) \to \max \\ T_{рек}\left(\{p^k(z), p^r(z)\}, u_j, o_b\right) \le T_{доп} \\ Q_{рек}\left(\{p^k(z), p^r(z)\}, u_j, f_d, o_b\right) \ge Q^*_{доп} \end{cases}, \qquad (14)$$

где $o_a \in O = [o_1, o_2, \ldots, o_H]$ – множество методов проведения процедуры реконфигурации в САС; $T_{рек}\left(\{p^k(x), p^r(x)\}, u_j, o_b\right)$ – временные затраты на выполнение процедура аутентификации при использовании o_b –го метода реконфигурации; $Q_{рек}\left(\{p^k(x), p^r(x)\}, u_j, f_d, o_b\right)$ – размер запросных и ответных сигналов САС; $Q^*_{доп}$ – минимально возможная разрядность запросных и ответных сигналов при постепенной деградации структуры САС.

Результаты исследования и их обсуждение

Рассмотрим разработанную методику построения отказоустойчивой САС, функционирующей в кодах ПСКВ.

1 этап. Проведенные исследования показали, что среди методов аутентификации особое место занимают протоколы, базирующиеся на доказательстве с нулевым разглашением [12-15]. В настоящее время наибольшее распространение получили протоколы аутентификации Фиат-Шамира, Фейге-Фиат-Шамира. Однако обладая высокой имитостойкостью, такие протоколы требует несколько раундов выполнения процедур типа «запрос – ответ», что не позволяет их использовать в САС из-за низкой скорости опознавания спутника. Данного недостатка лишен протокол аутентификации с нулевым разглашением, представленный в работе [3]. Для

реализации данного протокола требуется минимальное число этапов по сравнению с ранее известными протоколами. Кроме того, в его основе используются операции сложения, вычитания и умножения по модулю, эффективно выполняемые в ПСКВ. Данный протокол содержит следующие этапы:

Предварительный этап

Перед началом работы САС система получает секретные параметры: ключ спутника K, два числа S и T, которые предназначены для вычисления сеансовых ключей S(j) и проверки повторного применения данного ключа T(j). Для выполнения данного протокола в коде ПСКВ в качестве порождающего элемента группы выбирают $g(x)=x$. После этого определяется истинный статус спутника:

$$C^j(x)=\left(\left|g(x)^{K_1}\,g(x)^{S_1^j}\,g(x)^{T_1^j}\right|^{+}_{p_i(x)},\ldots,\left|g(x)^{K_k}\,g(x)^{S_k^j}\,g(x)^{T_k^j}\right|^{+}_{p_i(x)}\right), \quad (15)$$

где $p_i(x)$ – полиномы ПСКВ; $K=(K_1\,||\,K_2\,||\ldots||\,K_k)$, $S^j=(S_1^j\,||\,S_2^j\,||\ldots||\,S_k^j)$, $T^j=(T_1^j\,||\,T_2^j\,||\ldots||\,T_k^j)$; $K_i=\deg p_i(x)$, $S_i^j=\deg p_i(x)$; $T_i^j=\deg p_i(x)$; $i=1,2,\ldots,k$.

После этого вычислительное устройство ответчика, используя числа $\{\Delta K_i,\ \Delta S_i^j,\ \Delta T_i^j\}<2^{\deg p_i(x)}-1$, вычисляет новые параметры:

$$\tilde{K}_i^j=\left|K_i+\Delta K_i^j\right|^{+}_{2^{\deg p_i(x)}-1},\ \tilde{S}_i^j=\left|S_i^j+\Delta S_i^j\right|^{+}_{2^{\deg p_i(x)}-1},\ \tilde{T}_i^j=\left|T_i^j+\Delta T_i^j\right|^{+}_{2^{\deg p_i(x)}-1}. \quad (16)$$

Эти параметры для вычисления зашумленного статуса спутника:

$$\tilde{C}^j(x)=\left(\left|g(x)^{\tilde{K}_1^j}\,g(x)^{\tilde{S}_1^j}\,g(x)^{\tilde{T}_1^j}\right|^{+}_{p_i(x)},\ldots,\left|g(x)^{\tilde{K}_k}\,g(x)^{\tilde{S}_k^j}\,g(x)^{\tilde{T}_k^j}\right|^{+}_{p_i(x)}\right). \quad (17)$$

Процедура аутентификации низкоорбитального спутника

Для вычисления статуса спутника запросчиком осуществляется передача запросного слова, в качестве которого используется случайное число $d^j=(d_1^j,d_2^j,\ldots d_k^j)$, где $d_i^j\equiv d^j \bmod 2_i^{\deg p_i(x)}-1;\ i=1,2,\ldots,k$.

Получив запросное слово $d^j = (d_1^j, d_2^j, \ldots d_k^j)$, ответчик формирует сигнал ответчика, используя для этого выражения:

$$r_i^1(j) = \left|\widetilde{K}_i^j - d_i^j K_i^j\right|^+_{2^{\deg p_i(x)}-1},$$

$$r_i^2(j) = \left|\widetilde{S}_i^j - d_i^j S_i^j\right|^+_{2^{\deg p_i(x)}-1}, \qquad (18)$$

$$r_i^3(j) = \left|\widetilde{T}_i^j - d_i^j T_i^j\right|^+_{2^{\deg p_i(x)}-1}.$$

Сигнал ответчика, представляющий собой набор остатков в виде:

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

предается запросчику. Получив данный сигнал, запросчик преобразует его в код ПСКВ с помощью процедуры прямого преобразования. Операция проверки базируется на выполнении выражения:

$$Y_i^j(x) = \left|\left(C_i^j(x)\right)^{d_i^j} g(x)^{r_i^1} g(x)^{r_i^2} g(x)^{r_i^3}\right|^+_{p_i(x)}. \qquad (19)$$

Спутник получит статус «свой» только при выполнении условия:

$$\left\{Y_1^j(x) = \widetilde{C}_1^j(x), Y_2^j(x) = \widetilde{C}_2^j(x), \ldots, Y_k^j(x) = \widetilde{C}_k^j(x)\right\}. \qquad (20)$$

Таким образом, был выбран протокол аутентификации с нулевым разглашением сведений w_e, удовлетворяющий выражению (9).

2 этап. Для обеспечения высокой имитостойкости необходимо определить разрядность сигналов запросчика и ответчика, при выполнении условия (10). Положим, что разрядность составляет $Q_{доп} = 15$ бит. В качестве оснований кода ПСКВ выбираем полиномы $p_1(x) = x^5 + x^4 + x^3 + x + 1$, $p_2(x) = x^5 + x^4 + x^3 + x^2 + 1$, $p_3(x) = x^5 + x^3 + x^2 + x + 1$. Для обеспечения свойства отказоустойчивости необходимо ввести два избыточных основания ПСКВ $p_4(x) = x^5 + x^2 + 1$ и $p_5(x) = x^5 + x^3 + 1$. В этом случае код ПСКВ способен исправлять все ошибки кратности $N_{доп} = 1$.

3 этап. Для выбора алгоритма поиска и коррекции ошибок в кодах ПСКВ был осуществлен анализ работ [5-9,16]. Проведенные исследования показали, что условию (14) удовлетворяет алгоритм вычисления модульной свертки, представленный в работе [16]. Данный алгоритм базируется на выражении:

$$\begin{cases} \sigma_1(x) = y_{k+1}(x) \oplus \ddot{y}_{k+1}(x) = y_{k+1}(x) \oplus \left| \sum_{j=1}^{k} \lambda_j(x) y_j(x) \right|^{+}_{p_{k+1}(x)} \\ \sigma_2(x) = y_{k+2}(x) \oplus \ddot{y}_{k+2}(x) = y_{k+2}(x) \oplus \left| \sum_{j=1}^{k} \lambda_j(x) y_j(x) \right|^{+}_{p_{k+2}(x)} \end{cases}, \quad (21)$$

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

Для вычисления модульной свертки сначала определяется значение:

$$z_j(x) = y_j(x) M_j^{-1}(x) \bmod p_j(x), \quad (22)$$

где $\deg\left(y_j(x) M_j^{-1}(x) \bmod p_j(x)\right) < \deg p_j(x)$; $j = 1, 2, \ldots, k$.

После этого вычисляется:

$$z_j(x)\lambda_j(x) \bmod p_{k+s}(x) = \left(\left| y_j(x) M_j^{-1}(x) \right|^{+}_{p_j(x)} M_j(x) \right) \bmod p_{k+s}(x). \quad (23)$$

Комбинация ПСКВ не содержит ошибку при выполнении условия:

$$\ddot{y}_{k+s}(x) = \left| \sum_{j=1}^{k} \lambda_j(x) z_j(x) \right|^{+}_{p_{k+s}(x)} = y_{k+s}(x). \quad (24)$$

4 этап. Для обеспечения отказоустойчивости системы аутентификации спутника выбираем метод реконфигурации, который на основе обменных операций позволит сохранить работоспособное состояние САС за счет снижения размерности запросного и ответного сигнала до величины $Q^{*}_{доп} = 10$ разрядов.

Рассмотрим работу системы аутентификации спутника.

В качестве информационных оснований кода ПСКВ были выбраны полиномы $p_1(x)=x^5+x^4+x^3+x+1$, $p_2(x)=x^5+x^4+x^3+x^2+1$, $p_3(x)=x^5+x^3+x^2+x+1$. Согласно выражению (1) рабочий диапазон кода ПСКВ равен $P_k(x)=\prod_{i=1}^{3}p_i(x)=x^{15}+x^{11}+x^{10}+x^2+1=8C05$. Для обеспечения свойства отказоустойчивости введены два избыточных основания ПСКВ $p_4(x)=x^5+x^2+1$ и $p_5(x)=x^5+x^3+1$. В этом случае код ПСКВ способен исправлять все ошибки кратности $N_{доп}=1$. Выбор информационных и контрольных оснований удовлетворяет выражению (11). Тогда, согласно (4) полный диапазон кода ПСКВ будет равен:

$$P_n(x)=x^{25}+x^{23}+x^{22}+x^{21}+x^{19}+x^{18}+x^{16}+x^{14}+x^{11}+$$
$$+x^{10}+x^9+x^8+x^4+x^3+1=2ED4F19=49106713_{10}.$$

Пусть задан секретный ключ К = 1AF80F = 1767439, сеансовый ключ S(j)= 29007D = 2687101 и число для проверки повторного применения данного ключа T(j) = 4ECC99 = 5164185. Используя выражение (15) и представив секретные параметры в виде:

К = 00001 || 10101 || 11110 || 00000 || 01111 = 1 || 21 || 30 || 0 || 15,

S(j) = 00010 || 10011 || 10100 || 00011 || 11101 = 2 || 19 || 20 || 3 || 29,

T(j) = 00100 || 11101 || 10011 || 00100 || 11001 = 4 || 29 ||19 || 4 || 25,

определим истинный статус спутника:

$$C_1^j(x)=\left|g(x)^{K_1}\,g(x)^{S_1^j}\,g(x)^{T_1^j}\right|^{+}_{p_i(x)}=\left|x^1\cdot x^2\cdot x^4\right|^{+}_{p_{11}(x)}=x^4+x^3+x,$$

$$C_2^j(x)=\left|g(x)^{K_2}\,g(x)^{S_2^j}\,g(x)^{T_2^j}\right|^{+}_{p_2(x)}=\left|x^{21}\cdot x^{19}\cdot x^{29}\right|^{+}_{p_2(x)}=x^3+x^2+x,$$

$$C_3^j(x)=\left|g(x)^{K_3}\,g(x)^{S_3^j}\,g(x)^{T_3^j}\right|^{+}_{p_3(x)}=\left|x^{30}\cdot x^{20}\cdot x^{21}\right|^{+}_{p_3(x)}=x^4+x+1,$$

$$C_4^j(x)=\left|g(x)^{K_4}\,g(x)^{S_4^j}\,g(x)^{T_4^j}\right|^{+}_{p_4(x)}=\left|x^0\cdot x^3\cdot x^4\right|^{+}_{p_3(x)}=x^4+x^2,$$

$$C_5^j(x)=\left|g(x)^{K_5}\,g(x)^{S_5^j}\,g(x)^{T_5^j}\right|_{p_5(x)}^{+}=\left|x^{15}\cdot x^{29}\cdot x^{25}\right|_{p_3(x)}^{+}=x^3+x^2+1.$$

Затем ответчик, используя условие $\left\{\Delta K_i,\Delta S_i^j,\Delta T_i^j\right\}<31$, определяет числа $\Delta K^j=29\|4\|11\|10\|4,\Delta S^j=9\|7\|10\|1\|1,\Delta T^j=9\|6\|6\|5\|3$, которые предназначены для вычисления новых параметров согласно (16)

$$\tilde{K}_1^j=\left|K_1+\Delta K_1^j\right|_{31}^{+}=\left|1+20\right|_{31}^{+}=21,\ \tilde{K}_2^j=\left|21+4\right|_{31}^{+}=25,\ \tilde{K}_3^j=\left|30+11\right|_{31}^{+}=10,$$
$$\tilde{K}_4^j=\left|0+10\right|_{31}^{+}=10,\ \tilde{K}_5^j=\left|15+4\right|_{31}^{+}=19.$$

$$\tilde{S}_1^j=\left|S_1^j+\Delta S_1^j\right|_{31}^{+}=\left|2+9\right|_{31}^{+}=11,\ \tilde{S}_2^j=\left|19+7\right|_{31}^{+}=26,\ \tilde{S}_3^j=\left|20+10\right|_{31}^{+}=30,$$
$$\tilde{S}_4^j=\left|3+1\right|_{31}^{+}=4,\ \tilde{S}_5^j=\left|25+3\right|_{31}^{+}=28.$$

$$\tilde{T}_1^j=\left|T_1^j+\Delta T_1^j\right|_{31}^{+}=\left|4+9\right|_{31}^{+}=13,\ \tilde{T}_2^j=\left|29+6\right|_{31}^{+}=4,\ \tilde{T}_3^j=\left|19+6\right|_{31}^{+}=25,$$
$$\tilde{T}_4^j=\left|4+5\right|_{31}^{+}=9,\ \tilde{T}_5^j=\left|25+3\right|_{31}^{+}=28.$$

Используя выражение (17), получаем зашумленный статус спутника:

$$\tilde{C}_1^j(x)=\left|g(x)^{K_1}\,g(x)^{S_1^j}\,g(x)^{T_1^j}\right|_{p_i(x)}^{+}=\left|x^{21}\cdot x^{11}\cdot x^{13}\right|_{p_{11}(x)}^{+}=x^2+x.$$

$$\tilde{C}_2^j(x)=\left|g(x)^{K_2}\,g(x)^{S_2^j}\,g(x)^{T_2^j}\right|_{p_2(x)}^{+}=\left|x^{25}\cdot x^{26}\cdot x^{4}\right|_{p_{11}(x)}^{+}=x^3+x^2+1.$$

$$\tilde{C}_3^j(x)=\left|g(x)^{K_3}\,g(x)^{S_3^j}\,g(x)^{T_3^j}\right|_{p_3(x)}^{+}=\left|x^{10}\cdot x^{30}\cdot x^{25}\right|_{p_3(x)}^{+}=x^3.$$

$$\tilde{C}_4^j(x)=\left|g(x)^{K_4}\,g(x)^{S_4^j}\,g(x)^{T_4^j}\right|_{p_4(x)}^{+}=\left|x^{10}\cdot x^{4}\cdot x^{9}\right|_{p_3(x)}^{+}=x^3+x^2+x+1.$$

$$\tilde{C}_5^j(x)=\left|g(x)^{K_5}\,g(x)^{S_5^j}\,g(x)^{T_5^j}\right|_{p_5(x)}^{+}=\left|x^{19}\cdot x^{30}\cdot x^{28}\right|_{p_3(x)}^{+}=x^2+x.$$

Рассмотрим операцию поиска и коррекции ошибок в полученном значениях истинного статуса спутника. Для вычисления свертки получаем:

$$M_1^{123}(x)=p_2(x)p_3(x)=x^{10}+x^9+x^7+x^6+x^5+x^4+x^3+x+1;\ M_1^{-1}(x)=x^4+x^2+1;$$
$$M_2^{123}(x)=p_1(x)p_3(x)=x^{10}+x^9+x^4+x^3+1;\ M_2^{-1}(x)=x^4+x+1;$$
$$M_3^{123}(x)=p_1(x)p_2(x)=x^{10}+x^8+x^7+x^6+x^4+x^3+x^2+x+1;\ M_3^{-1}(x)=x^2+x+1.$$

Тогда константы свертки для $p_4(x)=x^5+x^2+1$ будут равны:

$$\lambda_1^4(x)=\left|M_1(x)\right|^+_{p_4(x)}=x^3+x+1;\ \lambda_2^4(x)=\left|M_2(x)\right|^+_{p_4(x)}=x^4+x;$$
$$\lambda_3^4(x)=\left|M_3(x)\right|^+_{p_4(x)}=x^4+x^3+x^2+1.$$

Для $p_5(x)=x^5+x^3+1$ получаем константы свертки:

$$\lambda_1^5(x)=\left|M_1(x)\right|^+_{p_5(x)}=x+1;\ \lambda_2^5(x)=\left|M_2(x)\right|^+_{p_5(x)}=x^4+x^2+x+1;$$
$$\lambda_3^5(x)=\left|M_3(x)\right|^+_{p_5(x)}=x^3+1.$$

Пусть проверки подвергается истинный статус, который не содержит ошибки $C^j(x)=(x^4+x^3+x\,||\,x^3+x^2+x\,||\,x^4+x+1||\,x^4+x^2\,||\,x^3+x^2+1)$.

Воспользуемся выражением (22). Тогда:

$$z_1(x)=\left|y_1(x)M_1^{-1}(x)\right|^+_{p_1(x)}=\left|(x^4+x^3+x)(x^4+x^2+1)\right|^+_{p_1(x)}=x^3+x,$$
$$z_2(x)=\left|y_2(x)M_2^{-1}(x)\right|_{p_2(x)}=\left|(x^3+x^2+x)(x^4+x+1)\right|^+_{p_2(x)}=x^2+x,$$
$$z_3(x)=\left|y_3(x)M_3^{-1}(x)\right|_{p_3(x)}=\left|(x^4+x+1)\cdot(x^2+x+1)\right|^+_{p_3(x)}=x^3.$$

Воспользуемся (23) и (24) и получим контрольные остатки:

$$\ddot{y}_4(x)=\left|\sum_{j=1}^{3}\lambda_j(x)z_j(x)\right|^+_{p_4(x)}=x^4+x^2,$$

$$\ddot{y}_5(x)=\left|\sum_{j=1}^{3}\lambda_j(x)z_j(x)\right|^+_{p_5(x)}=x^3+x^2+1.$$

Тогда, используя выражение (21), получаем, что истинный статус спутника, представленный в коде ПСКВ, не содержит ошибки, так как:

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

Пусть в процессе вычисления зашумленного статуса произошел отказ третьего основания ПСКВ, а глубина ошибки равна $\Delta\alpha_3(x)=x^3+1$. Значит, ошибочный остаток равен $\alpha_3^*(x)=\alpha_3(x)+\Delta\alpha_3(x)=x^3+(x^3+1)=1$. Тогда зашумленный статус: $\tilde{C}^*(x)=(x^2+x\,||\,x^3+x^2+1||1||\,x^3+x^2+x+1||\,x^2+x)$.

Воспользуемся выражением (22). Тогда:

$$z_1(x) = \left| y_1(x) M_1^{-1}(x) \right|^+_{p_1(x)} = \left| (x^2 + x)(x^4 + x^2 + 1) \right|^+_{p_1(x)} = x^3,$$

$$z_2(x) = \left| y_2(x) M_2^{-1}(x) \right|_{p_2(x)} = \left| (x^3 + x^2 + 1)(x^4 + x + 1) \right|^+_{p_2(x)} = x^3 + x^2 + x,$$

$$z_3(x) = \left| y_3(x) M_3^{-1}(x) \right|_{p_3(x)} = \left| 1 \cdot (x^2 + x + 1) \right|^+_{p_3(x)} = x^2 + x + 1.$$

Воспользуемся выражениями (23) и (24) и получим контрольные остатки:

$$\ddot{y}_4(x) = \left| \sum_{j=1}^{3} \lambda_j(x) z_j(x) \right|^+_{p_4(x)} = x^3 + x^2,$$

$$\ddot{y}_5(x) = \left| \sum_{j=1}^{3} \lambda_j(x) z_j(x) \right|^+_{p_5(x)} = x^4 + x^2 + x.$$

Тогда, получаем

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

Используя данное значение синдрома ошибки, выбирается вектор ошибки $e(x) = \Delta\alpha_3(x)$ и производится коррекция результата третьего остатка:

$$\alpha_3(x) = \alpha_3^*(x) + \bar{e}_3(x) = 1 + (x^3 + 1) = x^3.$$

Процедура аутентификации низкоорбитального спутника. Пусть запросчик выбрал запросное слово $d^j = (5 \| 2 \| 4 \| 28 \| 21)$.

Получив запросное слово $d^j = (5 \| 2 \| 4 \| 28 \| 21)$, ответчик формирует сигнал ответчика, используя для этого выражения (18). Тогда:

$$r_1^1(j) = \left| \tilde{K}_1^j + d_1^j K_1^j \right|^+_{31} = \left| 21 - 5 \cdot 1 \right|^+_{31} = 16, \; r_1^2(j) = \left| \tilde{S}_1^j + d_1^j S_1^j \right|^+_{31} = \left| 11 - 5 \cdot 2 \right|^+_{31} = 1,$$

$$r_1^3(j) = \left| \tilde{T}_1^j + d_1^j T_1^j \right|^+_{31} = \left| 13 - 5 \cdot 4 \right|^+_{31} = 24.$$

Аналогичным образом получаем остальные ответы:

$$r_2^1(j)=\left|\widetilde{K}_2^j+d_2^jK_2^j\right|_{31}^+=14,\ r_2^2(j)=\left|\widetilde{S}_2^j+d_2^jS_2^j\right|_{31}^+=19,\ r_2^3(j)=\left|\widetilde{T}_2^j+d_2^jT_2^j\right|_{31}^+=8,$$

$$r_3^1(j)=\left|\widetilde{K}_3^j+d_3^jK_3^j\right|_{31}^+=14,\ r_3^2(j)=\left|\widetilde{S}_3^j+d_3^jS_3^j\right|_{31}^+=12,\ r_3^3(j)=\left|\widetilde{T}_3^j+d_3^jT_3^j\right|_{31}^+=11,$$

$$r_4^1(j)=\left|\widetilde{K}_4^j+d_4^jK_4^j\right|_{31}^+=10,\ r_4^2(j)=\left|\widetilde{S}_4^j+d_4^jS_4^j\right|_{31}^+=13,\ r_4^3(j)=\left|\widetilde{T}_4^j+d_4^jT_4^j\right|_{31}^+=21,$$

$$r_5^1(j)=\left|\widetilde{K}_5^j+d_5^jK_5^j\right|_{31}^+=14,\ r_5^2(j)=\left|\widetilde{S}_5^j+d_5^jS_5^j\right|_{31}^+=8,\ r_5^3(j)=\left|\widetilde{T}_5^j+d_5^jT_5^j\right|_{31}^+=30.$$

Затем ответчик передает запросчику истинный статус, зашумленный статус и ответы на запросное слово. Получив данный сигнал, запросчик, используя выражение (19), проверяет статус спутника:

$$Y_1^j(x)=\left|\left(C_1^j(x)\right)^{d_1^j}g(x)^{r_1^1}g(x)^{r_1^2}g(x)^{r_1^3}\right|_{p_1(x)}^+=\left|(x^4+x^3+x)^5\cdot x^{16}\cdot x^1\cdot x^{24}\right|_{p_1(x)}^+=x^2+x,$$

$$Y_2^j(x)=\left|\left(C_2^j(x)\right)^{d_2^j}g(x)^{r_2^1}g(x)^{r_2^2}g(x)^{r_2^3}\right|_{p_2(x)}^+=\left|(x^3+x^2+x)^2x^{14}\cdot x^{19}\cdot x^8\right|_{p_2(x)}^+=x^3+x^2+1,$$

$$Y_3^j(x)=\left|\left(C_3^j(x)\right)^{d_3^j}g(x)^{r_3^1}g(x)^{r_3^2}g(x)^{r_3^3}\right|_{p_3(x)}^+=\left|(x^4+x+1)^4x^{14}\cdot x^{12}\cdot x^{11}\right|_{p_3(x)}^+=x^3,$$

$$Y_4^j(x)=\left|\left(C_4^j(x)\right)^{d_4^j}g(x)^{r_4^1}g(x)^{r_4^2}g(x)^{r_4^3}\right|_{p_4(x)}^+=\left|(x^4+x^2)^{28}x^{10}x^{13}\cdot x^{21}\right|_{p_4(x)}^+=x^3+x^2+x+1,$$

$$Y_5^j(x)=\left|\left(C_5^j(x)\right)^{d_5^j}g(x)^{r_5^1}g(x)^{r_5^2}g(x)^{r_5^3}\right|_{p_5(x)}^+=\left|(x^3+x^2+1)^{21}x^{14}\cdot x^8\cdot x^{30}\right|_{p_2(x)}^+=x^2+x.$$

Так как равенство (20) справедливо, то спутник имеет статус «свой», даже при возникновении одной ошибки из-за отказа вычислительного тракта, соответствующего третьему основанию ПСКВ.

Однако при возникновении второго отказа, например, первого основания, ответчик не сможет исправлять двукратную ошибку, но при наличии двух контрольных оснований – обнаружит ее. Пусть правильный истинный статус спутника имеет вид:

$$C^j(x)=(x^3+x^2+x\,||\,x^4+x+1\,||\,x^3+x+1\,||\,x^4+x^2\,||\,x^4+x^3+x^2+x+1).$$

В сложившейся ситуации будут искажены два остатка: первый и третий. Допустим, что глубина ошибки по первому основанию $\Delta\alpha_1(x)=x$, а по третьему основанию $\Delta\alpha_3(x)=x^3+1$. Тогда искаженный статус имеет вид:

$$C^*(x)=((x^3+x^2)^*\,||\,x^4+x+1||\,(x)^*\,||\,x^4+x^2\,||\,x^4+x^3+x^2+x+1).$$

В этом случае система аутентификации производит реконфигурацию. Для этого отключают третье основание ПСКВ. Тогда остаются два рабочих основания: $p_1(x)=x^5+x^4+x^3+x+1$, $p_2(x)=x^5+x^4+x^3+x^2+1$, а так же два избыточных основания: ПСКВ $p_4(x)=x^5+x^2+1$ и $p_5(x)=x^5+x^3+1$. Согласно выражению (1), рабочий диапазон кода ПСКВ составит $P_k^{1245}(x)=\prod_{i=1}^{2}p_i(x)=x^{10}+x^8+x^7+x^6+x^4+x^3+x^2++x+1$. В этом случае происходит уменьшение рабочего диапазона до предельного значения, равного 10 разрядам. Тогда истинный статус примет вид:

$$C^*(x)=((x^3+x^2)^*\,||\,x^4+x+1||\,\_\_\_\,||\,x^4+x^2\,||\,x^4+x^3+x^2+x+1)=$$
$$=((x^3+x^2)^*\,||\,x^4+x+1||\,x^4+x^2\,||\,x^4+x^3+x^2+x+1).$$

Чтобы реализовать процесс обнаружения и коррекции ошибок, производится пересчет ортогональных базисов для рабочих оснований, используя метод, приведенный в работе [9]. В этом случае получаем:

$$M_1^{12}(x)=p_2(x)=x^5+x^4+x^3+x^2+1.$$
$$M_2^{123}(x)=p_1(x)=x^5+x^4+x^3+x+1.$$

Воспользуемся таблицей 1, где приведены константы для вычисления веса ортогонального базиса [9]. Тогда веса ортогональных базисов равны:

$$M_1^{-1}=x^3+x+1,\ M_2^{-1}=x^3+x.$$

Тогда константы свертки для $p_4(x)=x^5+x^2+1$ будут равны:

$$\lambda_1^4(x)=\left|M_1^{12}(x)\right|^+_{p_4(x)}=x^4+x^3;\ \lambda_2^4(x)=\left|M_2^{12}(x)\right|^+_{p_4(x)}=x^4+x^3+x^2+x.$$

Для $p_5(x)=x^5+x^3+1$ получаем константы свертки:

$$\lambda_1^5(x)=\left|M_1^{12}(x)\right|^{+}_{p_5(x)}=x^4+x^2;\ \lambda_2^5(x)=\left|M_2^{12}(x)\right|^{+}_{p_5(x)}=x^4+x.$$

Проверке подвергается истинный статус:

$$C^*(x)=((x^3+x^2)^*\,||\,x^4+x+1||\,x^4+x^2\,||\,x^4+x^3+x^2+x+1).$$

Воспользуемся выражением (22). Тогда:

$$z_1(x)=\left|y_1(x)M_1^{-1}(x)\right|^{+}_{p_1(x)}=\left|(x^3+x^2)(x^3+x+1)\right|^{+}_{p_1(x)}=x,$$
$$z_2(x)=\left|y_2(x)M_2^{-1}(x)\right|_{p_2(x)}=\left|(x^4+x+1)(x^3+x)\right|^{+}_{p_2(x)}=x^3+x^2+1.$$

Воспользуемся выражениями (23) и (24) и получим контрольные остатки:

$$\ddot{y}_4(x)=\left|\sum_{j=1}^{3}\lambda_j(x)z_j(x)\right|^{+}_{p_4(x)}=x^4+x^2+x+1,$$
$$\ddot{y}_5(x)=\left|\sum_{j=1}^{3}\lambda_j(x)z_j(x)\right|^{+}_{p_5(x)}=x^4+x^2.$$

Тогда, используя выражение (21), получаем, что истинный статус спутника, представленный в коде ПСКВ, содержит ошибки, так как:

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

Используя данное значение синдрома ошибки, выбирается вектор ошибки $e(x)=\Delta\alpha_1(x)$ и производится коррекция результата первого остатка:

$$\alpha_1(x)=\alpha_1^*(x)+\bar{e}(x)=(x^3+x^2)+x=x^3+x^2+x.$$

Для оценки эффективности предложенных решений воспользуемся коэффициентом запаса работоспособности отказоустойчивой САС, определяемого выражением (13). Сравнительный анализ проведем с отказоустойчивой системой аутентификации спутника, использующей метод структурной избыточности «2 из 3», а также с САС, функционирующей в ПСКВ без реконфигурации структуры. Результаты анализа альтернативных

решений построения отказоустойчивых систем аутентификации спутника показаны на рис.2.

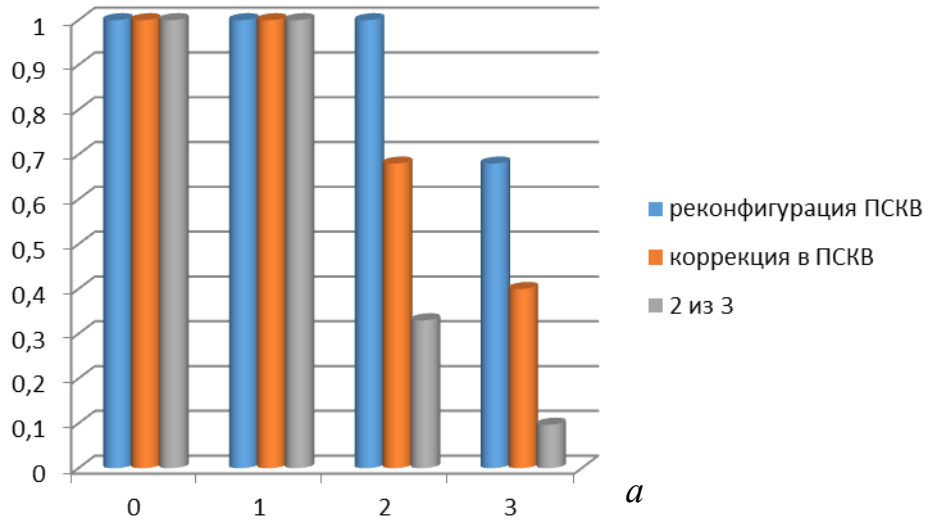

Рис. 2 Отказоустойчивость систем аутентификации спутника при накоплении отказов ($a = 1, 2, 3, \ldots$)

На основе анализа рис.2 можно сделать вывод о том, что использование метода реконфигурации структуры системы аутентификации спутника позволяет обеспечить работоспособное состояние САС даже при последовательном возникновении двух отказов за счет снижения в разрядности ответного и запросного слов. При этом метод структурной избыточности «2 из 3» и корректирующих кодов ПСКВ позволили обеспечить работоспособное состояние САС только при возникновении одного отказа. Таким образом, использование разработанной методики построения отказоустойчивой системы аутентификации низкоорбитальных спутников, функционирующей в полиномиальной системе классов вычетов, позволяет обеспечить более эффективную работу САС в условиях выхода множественных отказов в оборудовании.

Выводы

Коды ПСКВ обладают потенциальной возможностью динамически изменять такие показатели функционирования вычислительного устройства, как точность, информационную достоверность и производительность в режиме вычислений. Сделан вывод о целесообразности использования обменных операций в системах аутентификации спутника. Была разработана методика построения отказоустойчивой системы аутентификации низкоорбитальных спутников, функционирующей в полиномиальной системе классов вычетов. Показано, что, используя данную методику, можно разработать отказоустойчивую САС, которая за счет применения обменных операций может парировать несколько отказов, возникающих друг за другом, за счет постепенного снижения основных показателей качества функционирования в допустимых пределах. В рассмотренном примере САС остается в работоспособном состоянии даже при последовательном возникновении двух отказов за счет снижения в разрядности ответного и запросного слов. При этом метод структурной избыточности «2 из 3» и корректирующих кодов ПСКВ позволили обеспечить работоспособное состояние САС только при возникновении одного отказа.

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

Литература

1. Комаров И.А. РКС провел презентацию новой системы глобальной спутниковой связи. // URL: russianspacesystems.ru/2018/05/22/rks-provel-prezentaciyu-novoy-sistemy-efir

2. Щербань И.В., Толмачев С.А., Конев Д.С. Слабосвязанный алгоритм интегрированной инерциально-спутниковой навигационной системы транспортного средства // Инженерный вестник Дона, 2013, №3. URL: ivdon.ru/ru/magazine/archive/n3y2013/1821

3. Калмыков И.А., Чистоусов Н.К., Чипига А.Ф., Калмыков М.И., Павлюк Д.Н. Разработка метода аутентификации для обеспечения информационной скрытности низкоорбитальной группировки космических аппаратов // Инженерный вестник Дона, 2020, №4. URL: ivdon.ru/ru/magazine/archive/n4y2020/6416

4. Pashintsev V.P., Zhuk A.P., Kalmykov M.I., Olenev A.A. Redundant modular codes for development of fault-tolerant systems of satellite identification// International Journal of Emerging Trends in Engineering Research, 2020, 8(7), pp. 3160-3168.

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

6. Ananda Mohan Residue Number Systems. Residue Number Systems. Theory and Applications, 2016. 353 p.

7. Stepanova E.P., Makarova A.V. The use of redundant modular codes for improving the fault tolerance of special processors for digital signal processing // CEUR Workshop Proceedings. 1837, 2017. 418 p.

8. Chu J., Benaissa M. Polynomial residue number system GF(2m) multiplier using trinomials // In 17th European Signal Processing Conference. – Scotland, 2009. pp. 958-962.

9. Chu J., Benaissa M. Error detecting AES using polynomial residue number system // Microprocessors and Microsystems. 2013. № 37. pp. 228–234.

10. Степанова Е.П., Калмыкова Н.И., Павлюк Д.Н., Слюсарев Г.В. Разработка метода вычисления динамически изменяемого кортежа ортогональных базисов, позволяющего повысить отказоустойчивость системы опознавания спутника // Современные наукоемкие технологии. – 2020. № 4 (2). С. 223-227.

11. Надежность и эффективность в технике: Справочник / Ред. совет: Авдуевский В.С. (пред.) и др. – М.: Машиностроение, 1987. 237 с.

12. Молдовян А.А., Молдовян Д.Н., Левина А.Б. Протоколы аутентификации с нулевым разглашением секрета. СПб.: Университет ИТМО, 2016. – 55 с.

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

14. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. М.: Издательский центр «Академия», 2009. 272 с.

15. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2003. 816 с.

16. Калмыков И.А., Степанова Е.П., Павлюк Д.Н. Разработка алгоритма коррекции ошибок для повышения отказоустойчивости системы опознавания «свой-чужой» // Современные наукоемкие технологии. 2020. № 4. С. 19-25.

References

1. Komarov I.A. RKS provel prezentaciyu novoj sistemy global'noj sputnikovoj svyazi. [Russian space systems held a presentation of a new global satellite communication system]. URL: russianspacesystems.ru/2018/05/22/rks-provel-prezentaciyu-novoy-sistemy-efir

2. Shcherban I.V., Tolmachev S.A., Konev D.S. Inzhenernyj vestnik Dona, 2013, №3. URL: ivdon.ru/ru/magazine/archive/n3y2013/1821

3. Kalmykov I.A. Chistousov N.K., Chipiga A.F., Kalmykov M.I., Pavlyuk D.N. Inzhenernyj vestnik Dona, 2020, № 4.URL: ivdon.ru/ru/magazine/archive/n4y2020/6416.

4. Pashintsev V.P, Zhuk A.P., Kalmykov M.I., Olenev A.A. International Journal of Emerging Trends in Engineering Research, 2020, 8(7), pp. 3160-3168.

5. Sarkisov A.B., Rezenkov D.N., Gordenko D.V. Metody i algoritmy rekonfiguratsii nepozitsionnykh vychislitelnykh struktur dlya obespecheniya otkazoustoychivosti spetsprotsessorov [Methods and algorithms for reconfiguration of non-positional computing structures to ensure fault tolerance of special processors], Monografiya, Stavropol: Izdatelsko-informatsionnyy tsentr «Fabula», 2014, 180 p.

6. Ananda Mohan Residue Number Systems. Residue Number Systems. Theory and Applications, 2016. 353 p.

7. Stepanova E.P., Makarova A.V. The use of redundant modular codes for improving the fault tolerance of special processors for digital signal processing, CEUR Workshop Proceedings. 1837, 2017. 418 p.

8. Chu J., Benaissa M. In 17th European Signal Processing Conference, Scotland, 2009, pp. 958-962.

9. Chu J., Benaissa M. Error detecting AES using polynomial residue number system, Microprocessors and Microsystems, 2013, 37, pp. 228–234.

10. Stepanova E.P., Kalmykova N.I., Pavlyuk D.N., Slyusarev G.V. Sovremennyye naukoyemkiye tekhnologii, 2020, 4 (2), pp. 223-227.

11. Nadezhnost i effektivnost v tekhnike: Spravochnik [Reliability and efficiency in engineering: Handbook]. Red. sovet: Avduyevskiy V.S. (pred.) i dr., M.: Mashinostroyeniye, 1987, 237 p.

12. Moldovyan A.A., Moldovyan D.N., Levina A.B. Protokoly autentifikatsii s nulevym razglasheniyem sekreta [Authentication protocols with zero-knowledge of secret]. SPb.: Universitet ITMO, 2016, 55 p.

13. Zapechnikov S.V. Kriptograficheskiye protokoly i ikh primeneniye v finansovoy i kommercheskoy deyatelnosti [Cryptographic protocols and their application in financial and commercial activities], M.: Goryachaya liniya-Telekom, 2011, 256 p.

14. Cheremushkin, A.V. Kriptograficheskiye protokoly. Osnovnyye svoystva i uyazvimosti [Cryptographic protocol. Key features and vulnerabilities]. M.: Izdatelskiy tsentr «Akademiya», 2009, 272 p.

15. Shnayyer, B. Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnyye teksty na yazyke Si [Applied cryptography. Protocols, algorithms, and source texts in C]. M.: Izdatelstvo TRIUMF, 2003, 816 p.

16. Kalmykov I.A., Stepanova E.P., Pavlyuk D.N. Sovremennyye naukoyemkiye tekhnologii, 2020, №4, pp. 19-25.