

ПРИМЕНЕНИЕ ПОМЕХОУСТОЙЧИВОГО ПРОТОКОЛА АУТЕНТИФИКАЦИИ КОСМИЧЕСКОГО АППАРАТА ДЛЯ НИЗКООРБИТАЛЬНОЙ СИСТЕМЫ СПУТНИКОВОЙ СВЯЗИ

*Калмыков И.А., Калмыков М.И., Ляхов А.В., Пашинцев В.П.
Северо-Кавказский федеральный университет, Ставрополь, РФ
E-mail: pashintsevp@mail.ru*

В статье рассмотрены вопросы повышения имитостойкости и помехоустойчивости запросно-ответной системы опознавания «свой-чужой» для низкоорбитальной системы спутниковой связи за счет применения модулярных алгебраических систем.

Ключевые слова: низкоорбитальная спутниковая связь, запросно-ответная система, протокол аутентификации, полиномиальная система классов вычетов.

Введение

Разработка и добыча углеводородов в районах Крайнего Севера имеют стратегическое значение для становления экономики России. В этой связи непрерывно возрастает роль системы спутниковой связи (ССС), осуществляющей контроль, управление и мониторинг удаленных объектов с применением экологически опасных технологий в малонаселенных и труднодоступных областях Арктического побережья. При этом дестабилизация нормального функционирования ССС, вызванная как навязыванием ложных управляющих сигналов другими космическими аппаратами [1], так и искажениями передаваемых сигналов при их распространении через ионосферу в области полярных сияний [2], может привести к экологической катастрофе.

Поэтому повышение эффективности работы ССС за счет внедрения помехоустойчивого протокола аутентификации статуса спутника является актуальной задачей.

Постановка и решение задачи

В настоящее время крупные компании создают группировки космических аппаратов (КА), которые используются для организации бесперебойной и надежной связи с удаленными объектами управления нефтегазовой индустрии. Однако использовать геостационарные КА для управления удаленными объектами за пределами 81° с. ш. нельзя [1; 3]. Для этих целей создаются группировки низкоорбитальных КА. Основу таких группировок могут составлять космические аппараты «Ямал», «Гонец», «Сигнал» и т.д., которые используются для интерактивного дистанционного мониторинга объектов, располагаемых в районах

Крайнего Севера. Так как высота полета низкоорбитальных КА находится в пределах от 700 км до 1500 км, то для эффективного интерактивного контроля группировка должна содержать от 48 до 66 космических аппаратов [1; 3].

Время пролета низкоорбитального КА над абонентом может составлять всего 10-20 мин. Поэтому для таких КА характерна частая смена каналов передачи маркеров, сигнализации, синхронизации и информации. При этом возрастает вероятность того, что злоумышленник может осуществить попытку нарушения нормальной работы низкоорбитальной ССС путем имитации ложной управляющей информации (особенно на первом этапе передачи маркерных сигналов для определения входа КА в зону радиовидимости). Это, в свою очередь, приведет к дестабилизации функционирования системы мониторинга, контроля и управления объектами экологически опасных технологий, в результате которой может произойти авария оборудования. Последствия этого могут привести к частичному нарушению работы экосистемы Крайнего Севера.

Одним из путей решения данной проблемы является применение запросно-ответной системы опознавания «свой-чужой», способной в реальном масштабе времени определить статус КА, находящегося в зоне видимости абонентского терминала удаленного экологически опасного объекта. В [4-6] на основе проведенных исследований был предложен алгоритм работы системы опознавания «свой-чужой», использующий криптографический протокол аутентификации с нулевым доказательством. Следует отметить, что подобные протоколы эффективно используются в интерактивных информационных системах, где перед осуществлением диалога между двумя

субъектами каждый из них должен убедиться в соответствующем статусе другого. Примеры использования таких протоколов приведены в [6-8].

Целью статьи является повышение имитостойкости и помехоустойчивости запросно-ответной системы опознавания «свой-чужой» для низкоорбитальной системы спутниковой связи за счет применения модулярных алгебраических систем.

Алгоритм работы запросно-ответной системы опознавания статуса КА включает в себя следующие этапы.

Первый этап. В память ответчика, который располагается на борту КА, вводятся числа U – долгосрочный секретный ключ, S , T – база для вычисления сеансовых ключей $S(i)$ и $T(i)$. При этом используется разработанная псевдослучайная функция [9-11]. Тогда имеем

$$S(i) = g^{\frac{1}{\prod_j^{S_j+i+1}}} \bmod q, \quad (1)$$

$$T(i) = g^{\frac{1}{\prod_j^{T_j+i+1}}} \bmod q, \quad (2)$$

где q – мультипликативная группа; g – первообразный элемент этой группы; i – номер проводимого сеанса; j – номер двоичного блока при разбиении двоичного кода чисел S и T .

Второй этап. На основе этих данных U , $S(i)$ и $T(i)$ ответчик вычисляет истинный статус КА

$$C(i) = g^U g^{S(i)} g^{T(i)} \bmod q. \quad (3)$$

Третий этап. Затем производится зашумление данных U , $S(i)$ и $T(i)$, согласно

$$U^*(i) = U + \Delta U \bmod q, \quad (4)$$

$$S^*(i) = S(i) + \Delta S \bmod q, \quad (5)$$

$$T^*(i) = T(i) + \Delta T \bmod q, \quad (6)$$

где ΔU , ΔS , ΔT – величины зашумления.

Четвертый этап. На основе зашумленных данных вычисляется истинный статус КА

$$C^*(i) = g^{U^*} g^{S^*(i)} g^{T^*(i)} \bmod q. \quad (7)$$

Пятый этап. При появлении КА в зоне видимости запросчик, находящийся на абонентском терминале, генерирует «запросное число» d и пересылает его космическому аппарату.

Шестой этап. Получив «запросное число» d , ответчик вычисляет ответы

$$r_1 = U^* - dU \bmod \varphi(q), \quad (8)$$

$$r_2 = S(i)^* - dS(i) \bmod \varphi(q), \quad (9)$$

$$r_3 = T(i)^* - dT(i) \bmod \varphi(q). \quad (10)$$

Седьмой этап. Ответчик передает запросчику сигнал, который содержит вычисленный истинный статус $C(i)$, вычисленный зашумленный статус $C^*(i)$, ответы на вопрос r_1, r_2, r_3 .

Восьмой этап. Запросчик, получив данный сигнал, вычисляет результат

$$Y(i) = C^d(i) g^{r_1} g^{r_2} g^{r_3} \bmod q. \quad (11)$$

Если вычисленное значение $Y(i) = C^*(i)$, то принимается решение, что статус спутника «свой». В противном случае КА имеет статус «чужой».

Рассмотрим пример работы системы опознавания «свой-чужой». Пусть число, образующее мультипликативную группу, есть $q = 11$. В качестве порождающего элемента примем $g = 2$. Долговременный секретный ключ $U = 5$.

Для вычисления сеансовых ключей возьмем числа $S = 2$ и $T = 5$. Пусть номера сеанса будет первым, то есть $i = 1$. Представим в двоичном коде числа S , T и разобьем эти блоки на две части по 2 разряда в каждом. В этом случае получаем

$$S = 2_{10} = 0010_2; S_1 = 00_2 = 0_{10}, S_2 = 01_2 = 1_{10}, \\ T = 5_{10} = 0101_2; T_1 = 01_2 = 1_{10}, T_2 = 01_2 = 1_{10}.$$

Тогда первые сеансовые ключи равны

$$S(1) = g^{\frac{1}{\prod_j^{S_j+1+1}}} \bmod q = \left| 2^{((S_1+1+1)(S_2+1+1))^{-1}} \right|_{11}^+ =$$

$$= \left| 2^{(2^{-1}3^{-1})} \right|_{11}^+ = \left| 2^7 \right|_{11}^+ = 7;$$

$$T(1) = g^{\frac{1}{\prod_j^{T_j+1+1}}} \bmod q = \left| 2^{((T_1+1+1)(T_2+1+1))^{-1}} \right|_{11}^+ =$$

$$= \left| 2^{(9)^{-1}} \right|_{11}^+ = \left| 2^5 \right|_{11}^+ = 10.$$

На втором этапе происходит вычисление истинного статуса спутника

$$C(1) = g^U g^{S(1)} g^{T(1)} \bmod q = \\ = 2^5 \cdot 2^7 \cdot 2^{10} \bmod 11 = 4.$$

Полученное значение заносится в блок памяти ответчика, который располагается на борту КА. На третьем этапе происходит зашумление исход-

ных данных. Пусть в примере значения равны $\Delta U = 2$, $\Delta S = 6$, $\Delta T = 3$. Тогда получаем

$$\begin{aligned} U^* &= U + \Delta U \bmod q = (5 + 2) \bmod 11 = 7; \\ S^*(1) &= S(1) + \Delta S \bmod q = (7 + 6) \bmod 11 = 2; \\ T^*(1) &= T(1) + \Delta T \bmod q = (10 + 3) \bmod 11 = 2. \end{aligned}$$

Вычислим зашумленный образ спутника:

$$\begin{aligned} C^*(1) &= g^{U^*} g^{S^*(1)} g^{T^*(1)} \bmod q = \\ &= 2^7 \cdot 2^2 \cdot 2^2 \bmod 11 = 2. \end{aligned}$$

Вычисленное значение зашумленного статуса записывается в блок памяти КА.

Пусть запросчик, увидев спутник, посылает «запросное число», которое равно $d = 3$. Ответчик КА, получив «запросное число», осуществляет вычисление ответов

$$\begin{aligned} r_1 &= (7 - 3 \cdot 5) \bmod \varphi(q) = (7 - 15) \bmod 10 = 2; \\ r_2 &= (2 - 3 \cdot 7) \bmod \varphi(q) = (2 - 21) \bmod 10 = 1; \\ r_3 &= (2 - 3 \cdot 10) \bmod \varphi(q) = (2 - 30) \bmod 10 = 2. \end{aligned}$$

На шестом этапе алгоритма протокола ответчик передает запросчику сигнал, который содержит $C(1) = 4$, $C^*(1) = 2$, $r_1 = 2$, $r_2 = 1$, $r_3 = 2$.

На восьмом этапе протокола запросчик, получив данный сигнал, вычисляет результат согласно (11). Тогда

$$\begin{aligned} Y(1) &= C^d(1) g^{r_1} g^{r_2} g^{r_3} \bmod q = \\ &= 4^3 \cdot 2^2 \cdot 2^1 \cdot 2^2 \bmod 11 = 2. \end{aligned}$$

Таким образом, статус спутника – «свой».

Несмотря на то что представленный выше протокол с нулевым доказательством имеет высокую криптографическую стойкость (которая основывается на доказательстве о сложности решения λ -DDH проблемы), он характеризуется низкой помехоустойчивостью. Чтобы повысить ее, необходимо использовать корректирующие коды. Однако при этом требуется, чтобы помехоустойчивые коды использовали единую модулярную алгебраическую структуру совместно с предлагаемым протоколом и алгоритмами криптографической защиты, которые приведены в работах [10-13]. Такой подход позволит сократить схемные затраты на разработку программно-аппаратного комплекса, размещаемого на борту КА. Поэтому в работе предлагается использовать модулярные коды полиномиальной системы классов вычетов (ПСКВ), которые позволяют обнаруживать и исправлять ошибки, возникающие

из-за помех и искажений сигналов при передаче по каналу связи.

В ПСКВ в качестве оснований системы используются неприводимые полиномы $p_i(z)$, где $i = 1; 2 \dots n$. Произведение этих оснований определяет рабочий диапазон системы

$$P_{\text{раб}}(z) = \prod_{i=1}^n p_i(z). \quad (13)$$

В этом случае любой полином $A(z)$, удовлетворяющий условию

$$\deg A(z) < \deg P(z), \quad (14)$$

где $\deg A(z)$ – степень полинома $A(z)$, можно однозначно представить в виде набора остатков

$$A(z) = (\alpha_1(z), \alpha_2(z), \dots, \alpha_n(z)), \quad (15)$$

где $\alpha_i(z) \equiv A(z) \bmod p_i(z)$; $i = 1; 2 \dots n$.

Для реализации процесса обнаружения и исправления ошибок в модулярном коде полинома $A(z) = (\alpha_1(z); \alpha_2(z) \dots \alpha_n(z))$ вводят избыточность. Введение дополнительных контрольных оснований позволяет расширить диапазон системы до значения полного диапазона, определяемого как

$$P_{\text{полн}}(z) = \prod_{i=1}^{n+r} p_i(z) = P_{\text{раб}} \prod_{i=n+1}^{n+r} p_i(z), \quad (16)$$

где r – количество контрольных оснований. Избыточная кодовая комбинация ПСКВ $A(z) = (\alpha_1(z); \alpha_2(z) \dots \alpha_n(z); \alpha_{n+1}(z) \dots \alpha_{n+r}(z))$ считается разрешенной, то есть не содержит ошибок, если выполняется условие (14). В этом случае говорят, что непозиционный код принадлежит рабочему диапазону. В противном случае – комбинация ПСКВ содержит ошибки. Следовательно, для определения местоположения ошибки в кодовой комбинации $A(z)$ необходимо применять позиционные характеристики (ПХ). Применение ПХ позволяет определить местоположение проверяемой комбинации модулярного кода относительно рабочего диапазона системы.

Вопросам построения корректирующих модулярных кодов в настоящее время уделяется значительное внимание. Так, в [13] в качестве позиционной характеристики предлагается использовать интервальный номер комбинации, который определяется как

$$I_{\text{инт}}(z) = [A(z) / P_{\text{раб}}(z)]. \quad (17)$$

Так как операция деления (17) относится к немодульным операциям, то ее сводят к совокупности модульных операций. В работах [14-15] представлены алгоритмы, которые позволяют осуществлять поиск и коррекцию ошибки в коде классов вычетов, используя процедуры расширения системы оснований. В основу процедуры расширения системы оснований, базирующейся на вычислении синдрома ошибок по контрольным основаниям, положено определение разности между значениями остатков $\alpha_{n+1}(z); \alpha_{n+2}(z) \dots \alpha_{n+r}(z)$ по контрольным основаниям полинома $A(z) = (\alpha_1(z) \dots \alpha_{n+r}(z))$ и результатом вычисления остатков $\alpha'_{n+1}(z); \alpha'_{n+2}(z) \dots \alpha'_{n+r}(z)$ с использованием рабочих оснований. В математическом виде данный алгоритм можно представить как

рабочих оснований. В математическом виде данный алгоритм можно представить как

$$\begin{cases} \delta_{n+1}(z) = |\alpha_{n+1}(z) - \alpha'_{n+1}(z)|_{p_{n+1}(z)}^+ \\ \delta_{n+2}(z) = |\alpha_{n+2}(z) - \alpha'_{n+2}(z)|_{p_{n+2}(z)}^+ \\ \vdots \\ \delta_{n+r}(z) = |\alpha_{n+r}(z) - \alpha'_{n+r}(z)|_{p_{n+r}(z)}^+ \end{cases}, \quad (18)$$

$$\alpha'_j(z) = f(\alpha_1(z) \dots \alpha_n(z)); j = (n+1); \dots (n+r);$$

где f – алгоритм вычисления остатков по рабочим основаниям.

В [16-17] представлен алгоритм поиска и коррекции ошибок с использованием позиционной характеристики – коэффициентов обобщенной полиадической системы (ОПС). Данные алгоритмы основаны на вычислении коэффициентов промежуточной полиадической системы, в которой $A(z)$ изображается в виде

$$A(z) = b_1(z) + b_2(z)p_1(z) + \dots + b_{n+r}(z)p_1(z)p_2(z)\dots p_{n+r-1}(z). \quad (19)$$

где b_i – коэффициенты ОПС; $i = 1; 2 \dots (n+r)$.

Если полиномы $p_1(z); p_2(z) \dots p_{n+r}(z)$ служат одновременно основаниями ПСКВ и ОПС, то интервалы изменения цифр разрядов с одинаковыми номерами совпадут. Следовательно, если обеспечить соответствие между основаниями ОПС и основаниями системы классов вычетов, то справедливо

$$A = (\alpha_1(z), \alpha_2(z), \dots, \alpha_{n+r}(z)) = [b_1(z), b_2(z), \dots, b_{n+r}(z)] \quad (20)$$

Исходя из условия, что $P_{pa\bar{o}} = \prod_{i=1}^n p_i(z)$, выражение (19) примет вид

$$A(z) = b_1(z) + \dots + b_{n+1}(z)P_{pa\bar{o}}(z) + \dots + b_{n+r}(z)P_{pa\bar{o}}(z)p_{n+1}(z)\dots p_{n+r-1}(z). \quad (21)$$

На основании (21) делается следующий вывод: если полином $A(z)$ принадлежит рабочему диапазону $P_{pa\bar{o}}(z)$, то старшие коэффициенты ОПС, соответствующие контрольным основаниям, должны равняться нулю

$$b_{n+1}(z) = 0, b_{n+2}(z) = 0, \dots, b_{n+r}(z) = 0 \quad (22)$$

В противном случае полином $A(z)$ содержит ошибку и находится вне рабочего диапазона системы ПСКВ.

Однако рассмотренные выше алгоритмы характеризуются значительными схемными и временными затратами. В работе предлагается алгоритм, который позволяет осуществлять коррекцию ошибок при минимальной избыточности. С этой целью выбирается одно контрольное основание $p_{n+1}(z)$, удовлетворяющее условию

$$\deg p_{n+1}(z) \geq \deg p_n(z). \quad (23)$$

В этом случае используем одно контрольное основание для вычисления двух проверочных остатков

$$\alpha_{n+1}(z) = \sum_{i=1}^n \alpha_i(z), \quad (24)$$

$$\alpha_{n+2}(z) = \sum_{i=1}^n (i(z)\alpha_i(z)) \bmod p_{n+1}(z), \quad (25)$$

где $i(z)$ – полиномиальная форма i -го порядкового номера, суммирование в (24) по модулю два. Полученные контрольные остатки позволяют однозначно исправить однократную ошибку. Под однократной ошибкой понимается искажение одного разряда в кодовой комбинации кода ПСКВ.

При реализации разработанного алгоритма происходит обработка n информационных остатков $\alpha_1(z) \div \alpha_n(z)$ и двух контрольных остатков $\alpha_{n+1}(z)$ и $\alpha_{n+2}(z)$. Для обнаружения ошибки в переданной кодовой комбинации вычисляются значения

$$\alpha_{n+1}^*(z) = \sum_{i=1}^n \alpha_i(z), \quad (26)$$

$$\alpha_{n+2}^*(z) = \sum_{i=1}^n (i(z)\alpha_i(z)) \bmod p_{n+1}(z). \quad (27)$$

Полученные значения $\alpha_{n+1}^*(z)$ и $\alpha_{n+2}^*(z)$ используются для вычисления синдрома ошибки согласно выражениям

$$\delta_1(z) = \alpha_{n+1}(z) \oplus \alpha_{n+1}^*(z), \quad (28)$$

$$\delta_2(z) = \alpha_{n+2}(z) \oplus \alpha_{n+2}^*(z), \quad (29)$$

где \oplus – суммирование по модулю два.

Если синдром ошибки $\delta_1(z) = 0$ и $\delta_2(z) = 0$, то данная комбинация не содержит ошибки. В противном случае, когда $\delta_1(z) \neq 0$ и $\delta_2(z) \neq 0$, принятая комбинация является запрещенной, то есть ошибочной. По величине $\delta_1(z)$ и $\delta_2(z)$ можно провести коррекцию однократной ошибки.

В таблице 1 приведены значения синдромов $\delta_1(z)$ и $\delta_2(z)$, а также соответствующие им константы ошибки для рабочих оснований

$$p_1(z) = z + 1, \quad p_2(z) = z^2 + z + 1;$$

$$p_3(z) = z^4 + z^3 + z^2 + z + 1$$

и контрольного основания $p_4(z) = z^4 + z + 1$.

Таблица 1. Синдромы ошибки в коде ПСКВ

$\delta_1(z)$	$\delta_2(z)$	Константа ошибки $\Delta_{\text{конст}}$
0	0	(0, 0, 0, 0, 0)
1	1	(1, 0, 0, 0, 0)
1	z	(0, 1, 0, 0, 0)
z	z^2	(0, z , 0, 0, 0)
1	$z + 1$	(0, 0, 1, 0, 0)
z	$z^2 + z$	(0, 0, z , 0, 0)
z^2	$z^3 + z^2$	(0, 0, z^2 , 0, 0)
z^3	$z^3 + z + 1$	(0, 0, z^3 , 0, 0)

Проведенные исследования показали, что использование разработанного алгоритма поиска ошибок позволяет исправить все однократные ошибки и до 80% двукратных ошибок, которые возникают при передаче данных между КА и абонентским терминалом удаленного экологически опасного объекта.

Выводы

Проведенный анализ предметной области показал целесообразность применения запросно-ответной системы определения статуса космического аппарата в ССС, используемых для

дистанционного мониторинга и управления удаленными экологически опасными объектами. При этом такая система должна обеспечивать требуемый уровень защиты передаваемых данных от несанкционированных действий и высокую помехоустойчивость. Для обеспечения высокой имитостойкости ССС между абонентским терминалом удаленного экологически опасного объекта и центром поддержки операций в работе предлагается использовать криптографический протокол с нулевым разглашением. При этом повышение помехоустойчивости передаваемых данных осуществляется с помощью избыточных модулярных кодов. Таким образом, применение разработанной псевдослучайной функции в новом протоколе запросно-ответной системы опознавания, а также избыточных кодов полиномиальной системы классов вычетов позволяет защитить оборудование удаленного объекта от деструктивных воздействий, повысить эффективность его работы и снизить вероятность выхода из строя.

Литература

1. Камнев В.Е., Черкасов В.В., Чечин Г.В. Спутниковые сети связи. М.: Альпина Паблишер, 2004. – 536 с.
2. Маслов О.Н., Пашинцев В.П. Структурно-физическая модель трансферного канала связи // ИКТ. Т.5, №3, 2007. – С.19-25.
3. Низкоорбитальная космическая система персональной спутниковой связи и передачи данных. Под ред. А.И. Галькевича. Тамбов: ООО «Изд-во Юлис», 2011. – 69 с.
4. Калмыков И.А., Вельц О.В., Калмыков М.И., Науменко Д.О. Алгоритм имитозащиты для систем удаленного мониторинга и управления критическими технологиями // Известия ЮФУ. Технические науки. №2 (151), 2014. – С. 181-187.
5. Калмыков И.А., Саркисов А.Б., Макарова А.В., Калмыков М.И. Расширение методов защиты систем электронной коммерции на основе модулярных алгебраических схем // Известия ЮФУ. Технические науки. №2 (151), 2014. – С. 218-225.
6. Калмыков И.А., Дагаева О.И., Науменко Д.О., Вельц О.В. Системный подход к применению псевдослучайных функций в системах защиты информации // Вестник СКФУ. №3 (32), 2012. – С. 26-34.
7. Калмыков И.А., Дагаева О.И. Новые технологии защиты данных в электронных коммерческих системах на основе использования

- псевдослучайной функции // Известия ЮФУ. Технические науки. №12 (137), 2012. – С. 218-224.
8. Калмыков И.А., Дагаева О.И. Применение системы остаточных классов для формирования псевдослучайной функции повышенной эффективности // Вестник СКФУ. №3 (32), 2012. – С. 26-31.
 9. Калмыков И.А., Пашинцев В.П., Вельц О.В., Калмыков М.И. Методы защиты передаваемой информации для систем удаленного контроля и управления высокотехнологическими объектами // Вестник СКФУ. №4 (43), 2014. – С. 38-43.
 10. Калмыков И.А., Кихтенко О.А., Барильская А.В., Дагаева О.И. Криптографическая система на базе непозиционных полиномиальных алгебраических структур // Вестник СКФУ. №2, 2010. – С. 51-57.
 11. Калмыков И.А., Чипига А.Ф., Кихтенко О.А., Барильская А.В. Криптографическая защита данных в информационных технологиях на базе непозиционных полиномиальных систем // Известия ЮФУ. Технические науки. Т.100, № 11, 2009. – С. 210-220.
 12. Калмыков И.А., Чипига А.А. Алгоритм обеспечения информационной скрытности для адаптивных средств передачи информации // ИКТ. Т.5, № 3, 2007. – С. 159-162.
 13. Гапочкин А.В., Калмыков М.И., Васильев П.С. Обнаружение и коррекция ошибки на основе вычисления интервального номера кода классов вычетов // Современные наукоемкие технологии. №6, 2014. – С. 9-14.
 14. Барсагаев А.А., Калмыков М.И. Алгоритмы обнаружения и коррекции ошибок в модулярных полиномиальных кодах // Международный журнал экспериментального образования. №3, 2014. – С. 103-107.
 15. Калмыков И.А., Резеньков Д.Н., Горденко Д.В., Саркисов А.Б. Методы и алгоритмы реконфигурации непозиционных вычислительных структур для обеспечения отказоустойчивости спецпроцессоров. Ставрополь: Фабула, 2014. – 180 с.
 16. Калмыков И.А. Метод пересчета коэффициентов обобщенной полиадической системы для спецпроцессоров с деградируемой структурой // Известия ЮФУ. Технические науки. №4 (48), 2005. – С. 35-42.
 17. Стрижков Н.С., Калмыков М.И. Алгоритм преобразования из модулярного кода в полиадическую систему оснований для систем обнаружения и коррекции ошибок // Международный журнал экспериментального образования. №3, 2014. – С. 127-132.

Получено 20.01. 2015

Калмыков Игорь Анатольевич, д.т.н., профессор Кафедры информационной безопасности автоматизированных систем (ИБАС) Северо-Кавказского федерального университета (СКФУ). Тел. 8-918-77-33-001. E-mail: kia762@yandex.ru

Пашинцев Владимир Петрович, д.т.н., профессор Кафедры ИБАС СКФУ. Тел. 8-918-741-33-16. E-mail: pashintsevp@mail.ru

Калмыков Максим Игоревич, аспирант СКФУ. Тел. 8-906-471-02-42. E-mail: kmi762@yandex.ru

Ляхов Алексей Владимирович, ассистент Кафедры ИБАС СКФУ. Тел. 8-962-400-33-87.

APPLICATION OF JAM-PROOF SPACECRAFT AUTHENTICATION PROTOCOL FOR LOW-ORBIT SATELLITE COMMUNICATION SYSTEM

*Kalmykov I.A., Kalmykov M.I., Lyakhov A.V., Pashintsev V.P.,
North-Caucasus Federal University, Stavropol, Russian Federation
E-mail: pashintsevp@mail.ru*

Nowadays low-orbit satellite communication systems are widely used for remote control and effective monitoring of environment dangerous objects. Here application of inquiry-response friend-or-foe identification system provides identification of the status of spacecraft placing over line-of-sight for subscriber terminal of remote environment dangerous object. Therefore, failure probability for environment dangerous technologies will be decreased due to blockage of false signals from foe spacecraft. Due to features of Extreme North conditions, low orbit satellite communication systems transmit signals over ionosphere Aurora region, and it can produce an additional distortions being also reason of environmental disaster. This work represents reliable authentication protocol for low-orbit spacecrafts and satellite communication systems that provide reducing the negative effects due to distorted and imposed data transmission.

Keywords: low-orbit satellite communication, inquiry-response system, authentication protocol, polynomial class systems of deductions.

DOI: 10.18469/ikt.2015.13.2.11.

Kalmykov Igor Anatolievich, Doctor of Technical Science, Professor of Department of Information Security of Automated Systems, Institute of Information Technologies and Telecommunications, North-Caucasus Federal University, Stavropol, Russian Federation. Tel. +79034163533. E-mail: kia762@yandex.ru

Kalmykov Maksim Igorevich, PhD-student, Department of Information Security of Automated Systems, Institute of Information Technologies and Telecommunications, North-Caucasus Federal University, Stavropol, Russian Federation. Tel. +79064710242. E-mail: kmi762@yandex.ru.

Lyakhov Aleksey Vladimirovich, Assistant of the Department of Information Security of Automated Systems, Institute of Information Technologies and Telecommunications, North-Caucasus Federal University, Stavropol, Russian Federation. Tel. +79624003387.

Pashintsev Vladimir Petrovich, Doctor of Technical Science, Professor of Department of Information Security of Automated Systems, Institute of Information Technologies and Telecommunications, North-Caucasus Federal University, Stavropol, Russian Federation. Tel. +78652944241. E-mail: pashintsevp@mail.ru.

References

1. Kamnev V.E., Cherkasov V.V., Chechin G.V. *Sputnikovyie seti svyazi* [Satellite communications networks]. Moscow, Alpina Publisher, 2004. 536 p.
2. Maslov O.N., Pashintsev V.P. Strukturno-fizicheskaya model transionosfernogo kanala svyazi [Structurally the physical analog of ionosphere the channel of connection]. *Infokommunikacionnye tehnologii*, 2007, vol. 5, no. 3, pp. 19-25.
3. Galkevich A.I., Vladimirov S.O., eds. *Nizkoorbitalnaya kosmicheskaya sistema personalnoy sputnikovoy svyazi i peredachi dannyih* [Low earth orbit space system of personal satellite communications and data communications]. Tambov, Yulis Publ., 2011. 169 p.
4. Kalmyikov I.A., Velts O.V., Kalmyikov M.I., Naumenko D.O. Algoritm imitozaschityi dlya sistem udalennogo monitoringa i upravleniya kriticheskimi tehnologiyami [Development of an algorithm imitation resistance for of remote monitoring and control critical technologies]. *Izvestiya Yuzhnogo federalnogo universiteta. Tehnicheskie nauki – Izvestiya SFedU. Engineering Sciences*, 2014, no. 2, pp. 181-187.
5. Kalmyikov I.A., Sarkisov A.B., Makarova A.V., Kalmyikov M.I. Rasshirenie metodov zaschityi sistem elektronnoy kommertsii na osnove modulyarnyih algebraicheskikh shem [Enhanced protection methods of electronic commerce on the basis of modular algebraic scheme]. *Izvestiya Yuzhnogo federalnogo universiteta. Tehnicheskie nauki – Izvestiya SFedU. Engineering Sciences*, 2014, no. 2, pp. 218-225.
6. Kalmyikov I.A., Dagaeva O.I., Naumenko D.O., Velts O.V. Sistemnyiy podhod k primeneniyyu psevdosluchaynyih funktsiy v sistemah zaschityi informatsii [A system approach to usage of pseudorandom function in the data protection systems]. *Vestnik Severo-Kavkazskogo federalnogo universiteta*, 2012 no. 3, pp. 26-34.
7. Kalmyikov I.A., Dagaeva O.I. Novyye tehnologii zaschityi dannyih v elektronnyih kommercheskih sistemah na osnove ispolzovaniya psevdosluchaynoy funktsii [New technologies of e-commerce systems data security based on the usage of pseudorandom function]. *Izvestiya Yuzhnogo federalnogo universiteta. Tehnicheskie nauki – Izvestiya SFedU. Engineering Sciences*, 2012, no. 12, pp. 218-224.
8. Kalmyikov I.A., Dagaeva O.I. Primenenie sistemyi ostatochnyih klassov dlya formirovaniya psevdosluchaynoy funktsii povyishennoy effektivnosti [Application of residual classes for the formation of a pseudorandom function with increased efficiency]. *Vestnik Severo-Kavkazskogo federalnogo universiteta*, 2012 no. 3, pp. 26-31.
9. Kalmyikov I.A., Pashintsev V.P., Velts O.V., Kalmyikov M.I. Metodyi zaschityi peredavaemoy informatsii dlya sistem udalennogo kontrolya i upravleniya vyisokotehnologicheskimi ob'ektami [Methods for the protection of transmitted information system remote monitoring and control high-tech objects]. *Vestnik Severo-Kavkazskogo federalnogo universiteta*, 2014, no. 4, pp. 38-43.
10. Kalmyikov I.A., Kihtenko O.A., Barilskaya A.V., Dagaeva O.I. Kriptograficheskaya sistema na baze nepozitsionnyih polinomialnyih algebraicheskikh struktur [Cryptographic system based on the polynomial nonpositional algebraic structures]. *Vestnik Severo-Kavkazskogo federalnogo universiteta*, 2010, no. 2, pp. 51-57.

11. Kalmyikov I.A., Chipiga A.F., Kihthenko O.A., Barilskaya A.V. Kriptograficheskaya zaschita dannykh v informatsionnykh tehnologiyah na baze nepozitsionnykh polinomialnykh system [Cryptographic protection of data in information technology on base nepozitsionnykh polynomial systems]. *Izvestiya Yuzhnogo federalnogo universiteta. Tehnicheskie nauki – Izvestiya SFedU. Engineering Sciences*, 2009, no. 11, pp. 210-220.
12. Kalmyikov I.A., Chipiga A.A. Algoritm obespecheniya informatsionnoy skryitnosti dlya adaptivnykh sredstv peredachi informatsii [Algorithm for information secrecy providing for adaptive data transfer facilities]. *Infokommunikacionnye tehnologii*, 2007, vol. 5, no. 3, pp. 159-162.
13. Gapochkin A.V., Kalmyikov M.I., Vasilev P.S. Obnaruzhenie i korrektsiya oshibki na osnove vyichisleniya intervalnogo nomera koda klassov vyichetov [Error correction in modular code based parallel algorithms trail]. *Sovremennyye naukoymkie tehnologii*, 2014, no. 6, pp. 9-14.
14. Barsagaev A.A., Kalmyikov M.I. Algoritmy obnaruzheniya i korrektsii oshibok v modulyarnykh polinomialnykh kodakh [Algorithms of detection and correction of errors in modular polynomial codes]. *Mezhdunarodnyy zhurnal eksperimentalnogo obrazovaniya*, 2014, no. 3, pp. 103-107.
15. Kalmyikov I.A., Rezenkov D.N., Gordenko D.V., Sarkisov A.B. *Metody i algoritmy rekonfiguratsii nepozitsionnykh vyichislitelnykh struktur dlya obespecheniya otkazoustoychivosti spetsprotsektorov* [Methods and algorithms of nonpositional reconfiguration computational structures to provide fault tolerance of special processors]. Stavropol, Fabula Publ., 2014. 180 p.
16. Kalmyikov I.A. Metod perescheta koeffitsientov obobschennoy poliadicheskoy sistemy dlya spetsprotsektorov s degradiruemoy strukturoy [Coefficients recalculation method for the polyadic-generalized system of special processors with degradable structure]. *Izvestiya Yuzhnogo federalnogo universiteta. Tehnicheskie nauki – Izvestiya SFedU. Engineering Sciences*, 2005, no. 4, pp. 35-42.
17. Strizhkov N.S., Kalmyikov M.I. Algoritm preobrazovaniya iz modulyarnogo koda v poliadicheskuyu sistemu osnovaniy dlya sistem obnaruzheniya i korrektsii oshibok [Algorithm for converting from the modular code the polyadic system bases for systems error detection and correction]. *Mezhdunarodnyy zhurnal eksperimentalnogo obrazovaniya*, 2014, no. 3, pp. 127-132.

Received 20.01.2015

УДК 621.397

КОДИРУЮЩЕЕ И ДЕКОДИРУЮЩЕЕ УСТРОЙСТВА СИСТЕМЫ ONM ДЛЯ СЖАТИЯ ЦИФРОВОГО ПОТОКА ВИДЕОДАНЫХ

Безруков В.Н.¹, Балобанов А.В.¹, Балобанов В.Г.²

¹Московский технический университет связи и информатики, Москва, РФ

²Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ

E-mail: balobanov@tvpsati.ru

В работе рассматривается способ сжатия цифрового потока видеосигнала в телевизионном канале связи и вопросы практической реализации системы ONM, приводятся схемы кодирующего и декодирующего устройств. Дается описание их работы и сравнительный анализ с существующими системами сжатия MPEG. Предлагаются методы, повышающие эффективность сжатия цифрового потока в телевизионном канале связи.

Ключевые слова: квантователь, предсказатель, энтропийное кодирование, определитель движения, мультиплексор, прореживание, сумматор.

Введение

В работе [1] рассмотрены основные принципы способа сжатия видеоданных в системе ONM [2]. В предложенном способе последовательность полей (полукадров) делится на группы. В группе есть поля трех типов: О-поля – изображения, играющие роль опорных при восстановлении

других изображений. Предсказание для них не формируется, используют внутрислоево кодирование; N-четные поля – изображения, кодируемые путем предсказания на основе предыдущего поля, используют межслоево кодирование, в результате которого образуется межстрочная разность двух соседних строк нечетного и четного полей; M-нечетные поля – кодируемые с предска-