19. *Khubaev G.N.* Protsessno-statisticheskiy podkhod k uchetu zatrat resursov pri otsenke (kal'kulyatsii) sebestoimosti produktsii i uslug: osobennosti realizatsii, preimushchestva [Process-statistical approach to cost accounting resources when estimating (costing) cost of products and services: implementation and benefits], *Voprosy ekonomicheskikh nauk* [Questions of Economic Sciences], 2008, No. 2, pp. 158-166.
20. *Krepkov I.M., Efimov E.N., Fomenko N.M.* Analiz i uchet riskov prodvizheniya Internet–proektov predpriyatiya [Analysis and risk-based promotion of Internet–projects of the enterprise], Vestnik MEI [MPEI Vestnik], 2010, No. 2, pp. 101-107.

Статью рекомендовал к опубликованию к.т.н. А.П. Лапсарь.

Ефимов Евгений Николаевич – Ростовский государственный экономический университет (РИНХ); e-mail: efimov46@mail.ru; 344002, г. Ростов-на-Дону, Большая Садовая, 69, комн. 306 а; тел.: 89525721917; кафедра информационных технологий и защиты информации; д.э.н.; профессор.

Efimov Evgeny Nikolaevich – Rostov state economic University; e-mail: efimov46@mail.ru; Rostov-on-don, 344002, Large Garden, 69, room 306 a; phone: +79525721917; the Department of information technologies and information protection; dr. of ec. sc.; professor.

УДК 631.8

И.А. Калмыков, Т.А. Гиш, М.И. Калмыков, Д.О. Науменко, А.В. Дунин

ТЕХНОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ НЕПОЗИЦИОННЫХ КОДОВ ДЛЯ СИСТЕМ УПРАВЛЕНИЯ УДАЛЕННЫМИ ОБЪЕКТАМИ

Для обеспечения эффективной работы системы мониторинга, контроля и управления удаленными экологически опасными объектами в настоящее время широко используются системы спутниковой связи. Введение в состав абонентского терминала управления удаленным объектом запросно-ответной системы опознавания спутника позволит программно-аппаратному комплексу перед организацией информационного обмена произвести определение статуса космического аппарата, который находится в зоне видимости. В этом случае использование системы определения «свой-чужой» позволит снизить вероятность отказов и сбоев в процессе функционирования оборудования экологически опасных технологий из-за навязывания ложных управляющих команд, поступающих от чужих космических аппаратов. Для повышения эффективности работы запросно-ответной системы в работе предлагается использовать протокол с нулевым разглашением. Однако в процессе обмена данными между спутником и объектом управления может возникнуть ситуация перехвата, модификации и навязывания ложной информации. Для обеспечения высокой степени защиты информации от несанкционированного доступа в работе предлагается использовать алгоритм шифрования, реализованный в полиномиальной системе классов вычетов. Целью работы является повышение криптозащищенности запросно-ответной системы, применение которой позволит снизить вероятность навязывания ложной информации.

Система опознавания «свой-чужой»; криптографический протокол аутентификации; псевдослучайная функция; модулярные алгебраические структуры; алгоритм шифрования; полиномиальная система классов вычетов.

I.A. Kalmykov, T.A. Gish, M.I. Kalmykov, D.O. Naumenko, A.V. Dunin

THE INFORMATION PROTECTION TECHNOLOGY USING NON-POSITIONAL CODES FOR CONTROL SYSTEMS REMOTE OBJECTS

To ensure the effective operation of the system monitoring framework, monitoring and control of remote ecologically dangerous objects at the present time widely used satellite communication systems. The introduction of the subscriber terminal control of a remote object challenge-

response system of identification of the satellite will enable the hardware-software complex to the organization of information exchange to produce the definition of the status of the spacecraft, which is within sight. In this case, the use of the system identify "friend or foe" will decrease down the probability of faults and failures in the functioning of the equipment ecologically dangerous technologies from imposing false governors, coming from alien spacecraft. To improve the EF-performance, the challenge-response system it is proposed to use the Protocol with zero disclosure. However, in the process of communication between the satellite and the object to manage the situation may arise interception, modification and imposing false information. To ensure a high level of protection of information from unauthorized access, it is proposed to use the algorhythm encryption, implemented in polynomial system classes deductions. The aim of this work is to increase cryptotanshinone challenge-response system, which will reduce the probability of imposing false information.

System identification "friend or foe"; cryptographic authentication protocol; a pseudo-random function; modular algebraic structures; the encryption algorithm; polynomial class system of deductions.

Актуальность. В современных комплексах дистанционного мониторинга и управления удаленными экологически опасными объектами Крайнего Севера широко применяются системы спутниковой связи (ССС). По мере освоения месторождений Крайнего Севера число таких группировок будет только возрастать. В результате этого может возникнуть ситуация, связанная с попыткой нарушить нормальную работу системы спутниковой связи путем навязывания ложной управляющей информации, что может привести к экологической катастрофе. Поэтому задача повышения имитостойкости низкоорбитальной ССС за счет применения модулярных алгебраических систем является актуальной.

Метод решения. Несмотря на тяжелую сложившуюся ситуацию в экономике страны, вводимые зарубежными странами санкции, руководство Российской Федерации продолжает политику осваивания арктических территорий. Это связано с тем, что добываемые в районах Крайнего Севера углеводороды имеют стратегическое значение для развития и становления экономики РФ. При этом добыча и транспортировка углеводородных ископаемых осуществляется в малонаселенных и труднодоступных областях Арктического побережья.

В этих условиях роль операций, связанных с контролем, управлением, мониторингом и связью с удаленными объектами экологически опасных технологий постоянно возрастает. Техническая и программная реализация таких процедур переходит в ранг критических и первостепенных элементов в нефтегазовой индустрии, так как становится необходимым для обеспечения безопасности персонала, бесперебойной работы оборудования и повышения эффективности работы [1].

Для достижения поставленных целей современные компания стараются объединить навыки и компетенции высококвалифицированных специалистов с наиболее продвинутыми и развитыми технологическими процессами в области добычи и транспортировки углеводородов. Для этого формируются центры поддержки операций (ЦПО), основу которых составляют программное и аппаратное обеспечение, используемое при контроле добычи и транспортировки сырья, системы спутниковой связи (ССС), обеспечивающие в реальном масштабе времени обмен телеметрическими сведениями, результатами измерений соответствующих показателей и параметрами о ходе выполняемых работ. Такое сопровождение регистрируемых параметров позволяет обеспечить эффективное управление оборудованием, установленным на удаленном необслуживаемом объекте.

Однако, как показывает практика, для управления удаленными объектами, расположенными за пределами Полярного круга, нельзя использовать геостационарные орбитальные станции. Благодаря такому географическому положению месторождений углеводородов Крайнего Севера компании вынуждены создавать

группировки низкоорбитальных космических аппаратов. Для решения задач, связанных с интерактивным дистанционным мониторингом объектов, располагаемых за пределами Полярного круга, были разработаны и запущены космические аппараты «CRyoSat» и «Гонец» [2, 3]. Так как высота полета таких спутников находится в пределах от 800 до 1000 км, то для эффективного интерактивного контроля группировка должна содержать от 6 до 8 космических аппаратов.

Очевидно, что по мере освоения месторождений Крайнего Севера число таких группировок будет только возрастать. Это может привести к ситуации, когда злоумышленник может осуществить попытку нарушить нормальную работу системы космической связи путем навязывания ложной управляющей информации. В результате дестабилизация нормального функционирования системы спутниковой связи, используемой при мониторинге, контроле и управлении экологически опасными объектами, может вызвать экологическую катастрофу, что может привести к частичному нарушению работы экосистемы Ледовитого океана, а может быть, и полному уничтожению фауны Арктического побережья. Поэтому повышение эффективности работы ССС за счет применения новых технологий защиты информации с использованием непозиционных кодов, является актуальной задачей.

Целью данной статьи является повышение имитостойкости низкоорбитальной системы спутниковой связи за счет применения модулярных алгебраических систем.

Выбор модулярных алгебраических структур, обладающих свойством кольца и поля, обусловлен тем, что они в настоящее время нашли широкое применение в разных сферах. В работах [4–6] представлены алгоритмы и методы реализации цифровой обработки сигналов (ЦОС) с использованием непозиционных кодов. Малоразрядность обрабатываемых остатков, а также параллельный характер вычислений позволяют осуществлять цифровую обработку сигналов в реальном масштабе времени. Кроме того модулярные алгебраические системы, обладающие свойством кольца и поля, широко применяются в криптографии. В работах [7–9] представлены реализации псевдослучайных функций (ПСФ) с использованием модулярной арифметики. В результате были получены ПСФ, обладающие ℓ-DDH криптостойкостью при меньшей длине ключа. Также непозиционные коды способны обнаруживать и исправлять ошибки, которые возникают в процессе функционирования спецпроцессоров (СП). В работах [10, 11] представлены математические основы построения корректирующих непозиционных кодов. Невозможность распространения ошибки между параллельно работающими вычислительными трактами позволяет осуществлять обнаружение и исправление ошибок в процессе работы как криптографических СП, так и спецпроцессоров цифровой обработки сигналов.

Рассмотрим применение разработанной технологии защиты информации с использованием непозиционных кодов для систем управления удаленными объектами. Одним из перспективных направлений, которое позволяет достичь данную цель, является применение запросно-ответной системы, способной в реальном масштабе времени определить статус космического аппарата, находящегося в зоне видимости абонентского терминала управления удаленным экологически опасным объектом. В работе [12] на основе проведенных исследований был предложен алгоритм работы системы опознавания «свой-чужой». В основу алгоритма работы этой системы авторы предложили положить криптостойкий протокол с нулевым разглашением. Следует отметить, что подобные протоколы эффективно используются в интерактивных информационных системах, где перед осуществлением диалога между двумя субъектами, каждый из которых должен убедиться в соответствующем статусе другого. Примеры использования таких протоколов приведены в работах [13–15].

Рассмотрим на примере алгоритм работы запросно-ответной системы опознавания статуса спутника. На первом этапе работы выбирается модуль – простое число q, которое образует мультипликативную группу. Пусть число q = 11. Затем необходимо выбрать первообразный элемент мультипликативной группы g. В качестве такого первообразного элемента возьмем число g = 2. Пусть в качестве значения долговременного секретного ключа используется число U = 5.

Так как в процессе работы опознавания «свой-чужой» для обеспечения высокой степени имитозащиты необходимо постоянно менять сеансовые ключи, то для этой цели предлагается использовать псевдослучайную функцию, представленную в работах [7, 8]. Эта функция имеет следующий вид:

$$F((S_1,...,S_n),(g,T_1,...,T_n)) = g^{\left(\prod_{i=1}^{n}(S_i+T_i)\right)^{-1}} \bmod q, \quad (1)$$

где g – первообразный элемент мультипликативной группы; $(S_1,...,S_n)$ и $(T_1,...,T_n)$ – сеансовые ключи.

Для вычисления сеансовых ключей возьмем числа S = 2 и T = 5. При этом будем использовать выражения

$$S(i) = g^{\overline{\prod_j^{1} S_j+i+1}} \bmod q, \quad (2)$$

$$T(i) = g^{\overline{\prod_j^{1} T_j+i+1}} \bmod q, \quad (3)$$

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

Пусть номер сеанса будет первым, т.е. i = 1. Представим его в двоичной коде i =0001_2 . Аналогичным образом представим число = 2 =0010_2, а также число T = 5 = 0101_2. Пусть четырехразрядные двоичные значения S и T разбиваются 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, согласно (2) и (3), равны

$$S(1) = g^{\overline{\prod_j^{1} S_j+1+1}} \bmod q = 2^{\left((S_1+1+1)(S_2+1+1)\right)^{-1}} \bmod 11 = 2^{\left((0+1+1)(1+1+1)\right)^{-1}} \bmod 11 =$$

$$= 2^{(8)^{-1}} \bmod 11 = 2^7 \bmod 11 = 7$$

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

$$= 2^{(9)^{-1}} \bmod 11 = 2^5 \bmod 11 = 10$$

На втором этапе происходит вычисление истинного статуса спутника. При этом вычислительное устройство ответчика применяет значения *U, S(1)* и *T(1)* и используется выражение

$$C(i) = g^U g^{S(i)} g^{T(i)} \bmod q. \quad (4)$$

В приведенном примере значение истинного статуса космического аппарата будет равно

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

Полученное значение заносится в блок памяти ответчика, который располагается на борту КА.

На третьем этапе в вычислительном комплексе, используя полученные данные *U, S(1)* и *T(1),* производится их зашумление

$$U^* = U + \Delta U \, mod \, q, \tag{5}$$

$$S^*(i) = S(i) + \Delta S \bmod q, \tag{6}$$

$$T^*(i) = T(i) + \Delta T \bmod q, \tag{7}$$

где $\Delta U, \Delta S, \Delta T$ – величины зашумления значений *U, S(i)* и *T(i)* соответственно.

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

$$U^* = U + \Delta U \bmod q = (5+2) \bmod 11 = 7,$$

$$S^*(1) = S(1) + \Delta S \bmod q = (7+6) \bmod 11 = 2,$$

$$T^*(1) = T(1) + \Delta T \bmod q = (10+3) \bmod 11 = 2.$$

После этого вычислительное устройство ответчика вычисляет зашумленный статус космического аппарата согласно

$$C^*(i) = g^{U^*} g^{S^*(i)} g^{T^*(i)} \bmod q. \tag{8}$$

Таким образом, получаем зашумленный образ космического аппарата

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

Вычисленное значение зашумленного статуса записывается в блок памяти программно-аппаратного комплекса, размещенного на борту КА.

При появлении космического аппарата в зоне видимости станции космической связи запросчик, который находится на абонентском терминале удаленного объекта управления, генерирует «запросное число» *d* и пересылает его космическому аппарату. Пусть «запросное число» *d* = 3.

На следующем этапе, ответчик космического аппарата, получив «запросное число», осуществляет вычисление ответов

$$r_1 = U^* - dU \bmod \varphi(q), \tag{9}$$

$$r_2 = S(i)^* - dS(i) \bmod \varphi(q), \tag{10}$$

$$r_3 = T(i)^* - dT(i) \bmod \varphi(q), \tag{11}$$

В рассматриваемом примере получаем следующие ответы

$$r_1 = (7 - 3 \cdot 5) \bmod \varphi(q) = (7 - 15) \bmod 10 = 2,$$

$$r_2 = (2 - 3 \cdot 7) \bmod \varphi(q) = (2 - 21) \bmod 10 = 1,$$

$$r_3 = (2 - 3 \cdot 10) \bmod \varphi(q) = (2 - 30) \bmod 10 = 2.$$

На шестом этапе алгоритма протокола ответчик передает запросчику сигнал, который содержит:

- вычисленный истинный статус *C(1) = 4*;
- вычисленный зашумленный статус *C*(1) = 2*;
- ответы на поставленный вопрос $r_1 = 2, r_2 = 1, r_3 = 2$.

На седьмом этапе протокола запросчик, получив данный сигнал, вычисляет результат согласно

$$Y(i) = C^d(i) g^{r_1} g^{r_2} g^{r_3} \bmod q. \tag{12}$$

Если вычисленное значение *Y(i)* совпадет со значением зашумленного статуса космического аппарата, т.е. $Y(i) = C^*(i)$, то принимается решение, что статус спутника «свой». Между абонентским терминалом, представляющим собой про-

граммно-аппаратный комплекс, спроектированный на базе станции спутниковой связи, и КА производится обмен данными, которые являются результатом обработки навигационных и телеметрических данных на объекте мониторинга, и управляющими воздействиями, передаваемые с центра поддержки операций.

Если вычисленное значение *Y(i)* не совпадет со значением зашумленного статуса космического аппарата, т.е. $Y(i) \neq C^*(i)$, то принимается решение, что статус спутника «чужой» и обмен информацией между абонентским терминалом и КА не производится.

Для рассмотренного выше примера получаем, что результат проверки равен

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

Таким образом, статус спутника – свой.

Однако в процессе обмена данными между спутником и объектом управления может возникнуть ситуация перехвата, модификации и навязывания ложной информации. Для обеспечения высокой степени защиты информации от несанкционированного доступа необходимо использовать алгоритмы шифрования. При этом такой алгоритм криптозащиты должен быть реализован на основе алгебраической системы, обладающей свойством кольца и поля.

Одним из наиболее перспективных способов защиты информации является применение систем шифрования, использующие расширенные конечные поля $GF(2^v)$. Проведенные исследования показали, что такие системы обладают более широкими возможностями по реализации различных линейных и нелинейных криптографических функций [16-18]

$$A(z) + k(z) \equiv F(z) \bmod \pi(z), \quad (13)$$

$$A(z) k(z) \equiv F(z) \bmod \pi(z), \quad (14)$$

$$A(z)^{k(z)} \equiv F(z) \bmod \pi(z), \quad (15)$$

где $\pi(z)$ – неприводимый полином, порождающей поле $GF(q)$; $q = p^v$; p – простое число; $A(z)$ – блок открытого текста длиной v разрядов; $F(z)$ – блок зашифрованного текста длиной v разрядов; $\{k(z)\}$ – множество ключевых данных.

В работах [17, 18] представлен алгоритм нелинейного шифрования потока данных, использующий операцию возведения в степень символов конечного поля по модулю, согласно (15). Однако операция возведения элемента поля в степень трудоемка и требует больших затрат машинного времени. Применение полиномиальной системы классов вычетов (ПСКВ) позволяет сократить времени выполнения этого алгоритма. В данной непозиционной системе в качестве оснований используются неприводимые полиномы $p_i(z),\ i = 1, 2, ..., n$, произведение которых дает рабочий диапазон системы

$$P(z) = \prod_{i=1}^{n} p_i(z). \quad (16)$$

Как правило, в качестве основной области применения кодов полиномиальной системы классов вычетов выступает цифровая обработка сигналов. Это обусловлено тем, что за счет параллельной обработки малоразрядных данных повышается скорость выполнения ортогональных преобразований сигналов [19–22]. Данное свойство можно использовать для реализации процедур криптографической защиты информации. Рассмотрим алгоритм шифрования с использованием ПСКВ.

Для реализации алгоритма входной поток битов разбивается на отдельные блоки, двоичный код которых представляется в полиномиальной форме A(z). В этом случае размер блока выбирается из условия

$$\deg A(z) < \deg P(z). \quad (17)$$

Так как рабочий диапазон *P(z)* представляет собой кольцо неприводимых полиномов, то на основе изоморфизма, порожденного китайской теоремой об остатках, что каждый блок *A(z)*, можно однозначно представить в виде:

$$A(z) = (\alpha_1(z), \alpha_2(z), ..., \alpha_n(z)). \quad (18)$$

В этом случае выражение (15) можно представить следующим образом

$$F_j(z) = \left| A_j^{K_j}(z) \right|_{P(z)}^{+} = \left| (\alpha_1^j(z), \alpha_2^j(z), ..., \alpha_n^j(z))^{K_j} \right|_{P(z)}^{+} = (\beta_1^j(z), ..., \beta_n^j(z)), \quad (19)$$

где $\beta_i^j(z) \equiv F_j(z) \bmod p_i(z)$; $\alpha_i^j(z) \equiv A_j(z) \bmod p_i(z)$.

Так как сравнения по одному и тому же модулю можно почленно умножать, то последнее выражение представляется в виде:

$$F_j(z) = ((\alpha_1^j)^{K_j}(z), ..., (\alpha_n^j)^{K_j}(z)) \bmod P(z). \quad (20)$$

Рассмотрим пример. Пусть в качестве полиномов будут выбраны минимальные многочлены $p_1(z) = z+1$, $p_2(z) = z^3 + z^2 + 1$, $p_3(z) = z^3 + z + 1$. Рабочий диапазон расширенного поля Галуа GF(2^3) равен

$$P(z) = \prod_{i=1}^{3} p_i(z) = z^7 + 1.$$

Пусть задана двоичная последовательность двоичных битов

$$00111101100011000111 1.$$

Разобьем этот поток информации на 7-битовые блоки и представим их в полиномиальной форме. Тогда получаем

$$A_1(z) = 00111110 = z^4 + z^3 + z^2 + z;$$

$$A_2(z) = 1100011 = z^6 + z^5 + z + 1;$$

$$A_3(z) = 0001111 = z^3 + z^2 + z + 1.$$

Полученные полиномиальные значения переводим в код ПСКВ.

$$A_1(z) = z^4 + z^3 + z^2 + z = (0, z^2, z+1);$$

$$A_2(z) = z^6 + z^5 + z + 1 = (0, z^2 + z, 1);$$

$$A_3(z) = z^3 + z^2 + z + 1 = (0, z, z^2).$$

Разобьем двоичную ключевую последовательность на блоки по 3 бита каждый, а затем представим в десятичном коде

$$X = 100110111 = \{100, 110, 111, \ldots\} = \{4, 6, 7, \ldots\}.$$

Так как $7 \equiv 0 \bmod 2^3 - 1$, то его заменим на $p^{\nu} - 2 = 2^3 - 2 = 6$. Тогда последовательность показателей степеней, в которые необходимо возвести значение $A_j(z)$, представленных в модулярном коде ПСКВ, имеет вид

$$X^* = \{4, 6, 6, \ldots\}.$$

Выполним шифрование в ПСКВ первого блока $A_1(z)$. Получаем

$$F_1(z) = A_1^4(z) = (z^4 + z^3 + z^2 + z)^4 \bmod z^7 + 1 = z^5 + z^4 + z^2 + z = 0110110.$$

Переведем результат в модулярный код

$$\alpha_1(z) = A_1^4(z) \bmod p_1(z) = \left(z^5 + z^4 + z^2 + z\right) \bmod z + 1 = 0$$

$$\alpha_2(z) = A_1^4(z) \bmod p_2(z) = \left(z^5 + z^4 + z^2 + z\right) \bmod z^3 + z^2 + 1 = z$$

$$\alpha_3(z) = A_1^4(z) \bmod p_3(z) = \left(z^5 + z^4 + z^2 + z\right) \bmod z^3 + z + 1 = z^2 + z + 1.$$

Таким образом, первый блок открытого текста в ПСКВ представляется как

$$A_1^4(z) = z^5 + z^4 + z^2 + z = (0, z, z^2 + z + 1).$$

Реализуем нелинейное шифрование в модулярном коде

$$F_1(z) = A_1^4(z) = \left|(z^4 + z^3 + z^2 + z)^4\right|_{z^7+1}^{+} = (\left|0^4\right|_{z+1}^{+}, \left|(z^2)^4\right|_{z^3+z^2+1}^{+}, \left|(z+1)^4\right|_{z^3+z+1}) =$$

$$= (0,\ z,\ z^2 + z + 1).$$

Реализуем алгоритм (20) с остальными блоками открытого текста. Для второго блока открытых данных получаем

$$F_2(z) = A_2^6(z) = \left|(z^6 + z^5 + z + 1)^6\right|_{z^7+1}^{+} = z^6 + z^2.$$

Преобразуем в код ПСКВ данный результат

$$F_2(z) = A_2^6(z) = z^6 + z^2 = (0, z, 1).$$

Осуществим нелинейное шифрование с использованием ПСКВ

$$F_2(z) = A_2^6(z) = \left|(z^6 + z^5 + z + 1)^6\right|_{z^7+1}^{+} = (\left|0^6\right|_{z+1}^{+}, \left|(z^2 + z)^6\right|_{z^3+z^2+1}^{+}, \left|1^6\right|_{z^3+z+1}^{+}) =$$

$$= (0, z, 1).$$

Возведем в третью степень по модулю третий блок открытых данных

$$F_3(z) = A_3^6(z) = \left|(z^3 + z^2 + z + 1)^6\right|_{z^7+1}^{+} = z^4 + 1.$$

Полученный результат представим в коде ПСКВ

$$F_3(z) = A_3^6(z) = z^4 + 1 = (0, z^2 + z, z^2 + z + 1).$$

Проведем нелинейное шифрование в ПСКВ. Получаем

$$F_3(z) = A_3^6(z) = \left|(z^3 + z^2 + z + 1)^6\right|_{z^7+1}^{+} = (\left|0^6\right|_{z+1}^{+}, \left|z^6\right|_{z^3z^2+1}^{+}, \left|(z^2)^6\right|_{z^3+z+1}^{+}) =$$

$$= (0, z^2 + z, z^2 + z + 1).$$

Расшифрование принятого сообщения осуществляется

$$A_j(z) = \sqrt[K_j]{F_j(z)} \bmod P(z). \tag{21}$$

Тогда на основе изоморфизма КТО справедливо выражение

$$\alpha_i^j(z) = \sqrt[K_j]{\beta_i^j(z)} \bmod p_i(z), \tag{22}$$

где $\beta_i^j(z) \equiv F_j(z) \bmod p_i(z).$

Рассмотрим процедуру расшифрования, выполняемую также с использованием полиномиальной системы. Для выполнения выражений (21) и (22) необходимо определить мультипликативную обратную величину $(K_j)^{-1}$ относительно K_j по модулю $p^v - 1.$ В представленном примере для расширенного поля Галуа $GF(2^3)$ значения K^{-1} будут иметь следующий вид:

$$X^{-1} = \{2, 6, 6, \ldots\}.$$

Полученный первый блок $F_1(z)$ длиной 7 бит поступает на устройство, реализующее операцию дешифрования, согласно (21). При этом с выхода блока вы-

числения обратной мультипликативной величины подается значение $X_1^{-1} = 2$ в двоичном коде. В результате выполнения операции по модулю *P(z)* получаем

$$A_1(z) = \sqrt[4_1]{F_1(z)} \bmod P(z) = \left|(z^5 + z^4 + z^2 + z)^{-4_1}\right|^{+}_{z^7+1} = \left|(z^6 + z^5)^2\right|^{+}_{z^7+1} =$$

$$= z^4 + z^3 + z^2 + z = (0,\ z^2, z+1).$$

Расшифруем блок $F_1(z)$ в полиномиальной системе классов вычетов

$$A_1(z) = \sqrt[4_1]{(0, z^2+1, z)} \bmod P(z) = \left|(0, z, z^2+1)^2\right|^{+}_{z^7+1} =$$

$$= (\left|0^3\right|^{+}_{z+1}, \left|(z)^3\right|^{+}_{z^3+z^2+1}, \left|z^2+z+1\right|_{z^3+z+1}) = (0,\ z^2, z+1).$$

Проведем расшифрование блоков $F_2(z)$, $F_3(z)$. Для блока $F_2(z)$ получаем

$$A_2(z) = \sqrt[6]{F_2(z)} \bmod P(z) = \left|(z^6 + z^2)^{-x_2}\right|^{+}_{z^7+1} =$$

$$= \left|(z^6 + z^2)^6\right|^{+}_{z^7+1} = z^6 + z^5 + z + 1 = (0,\ z^2 + z, 1).$$

Реализуем расширование в полиномиальной системой класса вычетов

$$A_2(z) = \sqrt[6]{(0, z, 1)} \bmod P(z) = \left|(0, z, 1, z)^6\right|^{+}_{z^7+1} =$$

$$= (\left|0^6\right|^{+}_{z+1}, \left|z^6\right|^{+}_{z^3+z^2+1}, \left|1^6\right|_{z^3+z+1}) = (0,\ z^2 + z,\ 1).$$

Для третьего блока $F_3(z) = z^4 + 1$ получаем

$$A_3(z) = \sqrt[6]{F_3(z)} \bmod P(z) = \left|(z^4 + 1)^{-6}\right|^{+}_{z^7+1} =$$

$$= \left|(z^4 + 1)^6\right|^{+}_{z^7+1} = z^3 + z^2 + z + 1 = (0, z, z^2).$$

Воспользуемся полиномиальной системой класса вычетов. Тогда

$$A_3(z) = \sqrt[6]{F_3(z)} \bmod P(z) = 0, z^2 + z, z^2 + z + 1)^6 \bmod z^7 + 1 =$$

$$= (\left|0^6\right|^{+}_{z+1}, \left|(z^2 + z)^6\right|^{+}_{z^3+z^2+1}, \left|(z^2 + z + 1)^6\right|^{+}_{z^3+z+1}) = (0,\ z,\ z^2).$$

Теперь необходимо выполнить операцию обратного преобразования из модулярного кода ПСКВ в позиционный код. Для этого можно воспользоваться китайской теоремой об остатках или обобщенной полиадической системой.

Полученные результаты свидетельствуют о том, что при применении полиномиальной системы класса вычетов получается результат, аналогичный операции нелинейного шифрования с возведением в степень по модулю.

Проведем оценку криптографической стойкости разработанного алгоритма шифрования с использованием полиномиальной системы класса вычетов. Очевидно, что уровень криптографической защиты информации от несанкционированного доступа будет определяться всеми возможными отличающимися друг от друга вариантами выбора полных ключей. В этом случае для оценки криптографической стойкости разработанного алгоритма нелинейного шифрования воспользуемся равенством, определяющим вероятность вскрытия шифра

$$p_{kr} = \left(2^N \sum_{k_1, k_2, \ldots, k_s} \left((k_1 + k_2 + \ldots + k_s)! C_{n1}^{k1} C_{n2}^{k2} \ldots C_{ns}^{ks}\right)\right)^{-1}, \qquad (23)$$

где N – длина сообщения; s_i – количество неприводимых полиномов степени m_i; k_i – неизвестный коэффициент, выбираемый из условия $n = k_1 + k_2 + ... + k_s$; n – количество рабочих оснований ПСКВ.

Результаты определения криптостойкости представленного алгоритма нелинейного шифрования для сообщений, имеющих различные длины N, приведены в табл. 1.

Таблица 1

Криптостойкость алгоритма шифрования

Длина блока, бит	12	13	14	15	16
Криптостойкость алгоритм шифрования	$2*10^{-8}$	$4{,}9*10^{-8}$	$9*10^{-8}$	$2{,}4*10^{-9}$	$4{,}9*10^{-9}$

Анализ результатов показывает, что при длине блока открытого текста N=16 бит разработанный алгоритм нелинейного шифрования обеспечивает криптостойкость, сравнимую с величиной $4{,}9*10^{-9}$. При этом при увеличении разрядности обрабатываемых данных возрастает эффективность применения ПСКВ для реализации нелинейных криптографических процедур защиты данных от НСД. В ходе проведенных исследований выявлено, что применение полиномиальной системы классов вычетов для реализации нелинейного шифрования позволило снизить временные затраты более чем на 9 % по сравнению с выполнением метода шифрования с возведением в степень по модулю в поле Галуа $GF(2^3)$.

Заключение. Проведенный системный анализ предметной области показал целесообразность применения запросно-ответной системы определения статуса космического аппарата в системах спутниковой связи, используемых для дистанционного мониторинга и управления удаленными экологически опасными объектами. Для обеспечения высокой имитостойкости системы космической связи между абонентским терминалом удаленного экологически опасного объекта и центром поддержки операций в работе предлагается использовать криптографический протокол с нулевым разглашением. При этом защита передаваемых данных от НСД осуществляется с алгоритма нелинейного шифрования, реализованного в полиномиальной системе классов вычетов. Это позволило при длине блока открытого текста *N=16* бит обеспечить криптостойкость сравнимую с величиной $4{,}9*10^{-9}$. При этом использование алгебраических систем, обладающих свойством кольца и поля, позволило снизить временные затраты. Так при выполнении алгоритма шифрования с возведением в степень по модулю с использованием непозиционных кодов скорость шифрования повысилась более чем на 9 %. При этом, при увеличении разрядности обрабатываемых данных будет возрастать эффективность разработанной технологии защиты информации от НСД в системах управления удаленными объектами.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Центр поддержки операций компании Шлюмберже. http://www.slb.ru/page.php?code=28.
2. http://www.esa.int/Our_Activities/Observing_the_Earth/CryoSat.
3. *Галькевич А.И., Владимиров С.О., Дубровский В.М. и др.* Низкоорбитальная космическая система персональной спутниковой связи и передачи данных / Под ред. А.И. Галькевича. – Тамбов: ООО «Изд-во Юлис», 2011. – 169 с.
4. *Kalmykov I., Katkov K., Naumenko D., Sarkisov A., Makarova A.* Parallel Modular Technologies in Digital Signal Processing // Life Science Journal. – 2014. – № 11 (11s). – P. 435-438.
5. *Katkov K., & Kalmykov I.* Application of Parallel Technologies in Navigation Management under the Conditions of Artificial Ionospheric Disturbances // World Applied Sciences Journal. – 2013. – № 26 (1). – P. 108-113.

6. *Omondi A., & Premkumar B.* Residue number systems: theory and implementation. UK: Imperial College Press. 2007.
7. *Калмыков И.А., Дагаева О.И.* Новые технологии защиты данных в электронных коммерческих системах на основе использования псевдослучайной функции // Известия ЮФУ. Технические науки. – 2012. – №. 12 (137). – С. 218-224.
8. *Калмыков И.А., Дагаева О.И.* Применение системы остаточных классов для формирования псевдослучайной функции повышенной эффективности // Вестник Северо-Кавказского федерального университета. – 2012. – № 3 (32). – С. 26-31.
9. *Camenisch J., Gross T., & Sommer D.* Assertion message signatures. Patent US 8 341 416 B2. 2012. December 25.
10. *Agbedemnab P.A. and Bankas E.K.* A Novel RNS Overflow Detection and Correction Algorithm for the Moduli Set 2^n-1, 2^n, 2^n+1 // International Journal of Computer Applications (0975 – 8887). – January 2015. – Vol. 110, No. 16. – P. 30-34.
11. *Chu J., Benaissa M.* Error detecting AES using polynomial residue number system // Microprocessor and Microsystems. – 2013. – № 37. – P. 228-234.
12. *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 Северо-Кавказского федерального университета. – 2014. – № 4 (43). – С.38-43.
13. *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. – 2014. – № 2 (151). – С. 218-225.
14. *Калмыков И.А., Дагаева О.И., Науменко Д.О., Вельц О.В.* Системный подход к применению псевдослучайных функций в системах защиты информации // Вестник Северо-Кавказского федерального университета. – 2012. – № 3 (32). – С. 26-34.
15. *Wang Q.* Compact k-spendable E-cash with Anonymity Control Based Offline TTP // International Journal of Innovative Computing, Information and Control. – 2011. – № 7 (1). – С. 459-469.
16. *Калмыков И.А., Кихтенко О.А., Барильская А.В., Дагаева О.И.* Криптографическая система на базе непозиционных полиномиальных алгебраических структур // Вестник Северо-Кавказского федерального университета. – 2010. – № 2. – С. 51-57.
17. *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. – 2009. – № 11 (100). – С. 210-220.
18. *Калмыков И.А., Чипига А.А.* Алгоритм обеспечения информационной скрытности для адаптивных средст передачи информации // Инфокоммуникационные технологии. – 2007. – Т .5, № 3. – С. 159-162.
19. *Калмыков И.А., Калмыков М.И.* Структурная организация параллельного спецпроцессора цифровой обработки сигналов, использующего модулярные коды // Теория и техника радиосвязи. – 2014. – № 2. – С. 60-66.
20. *Бережной В.В., Калмыков, И.А. Червяков Н.И., Щелкунова Ю.О., Шилов А.А.* Нейросетевая реализация в полиномиальной системе классов вычетов операций ЦОС повышенной разрядности // Нейрокомпьютеры: разработка, применение. – 2004. – № 5-6. – С. 94.
21. *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.
22. *Барсагаев А.А, Калмыков М.И.* Алгоритмы обнаружения и коррекции ошибок в модулярных полиномиальных кодах // Международный журнал экспериментального образования. – 2014. – № 3-1. – С. 103-107.

REFERENCES

1. Tsentr podderzhki operatsiy kompanii Shlyumberzhe [Support center operations Schlumberger]. Available at: http://www.slb.ru/page.php?code=28.
2. http://www.esa.int/Our_Activities/Observing_the_Earth/CryoSat.
3. *Gal'kevich A.I., Vladimirov S.O., Dubrovskiy V.M. i dr.* Nizkoorbital'naya kosmicheskaya sistema personal'noy sputnikovoy svyazi i peredachi dannykh [Low-orbit space system of personal satellite communication and data transmission], Under ed. A.I. Gal'kevicha. Tambov: OOO «Izd-vo Yulis», 2011, 169 p.

4. *Kalmykov I., Katkov K., Naumenko D., Sarkisov A., Makarova A.* Parallel Modular Technologies in Digital Signal Processing, *Life Science Journal*, 2014, No. 11 (11s), pp. 435-438.
5. *Katkov K., & Kalmykov I.* Application of Parallel Technologies in Navigation Management under the Conditions of Artificial Ionospheric Disturbances, *World Applied Sciences Journal*, 2013, No. 26 (1), pp. 108-113.
6. *Omondi A., & Premkumar B.* Residue number systems: theory and implementation. UK: Imperial College Press. 2007.
7. *Kalmykov I.A., Dagaeva O.I.* Novye tekhnologii zashchity dannykh v elektronnykh kommercheskikh sistemakh na osnove ispol'zovaniya psevdosluchaynoy funktsii [New technologies of e-commerce systems data security based on the usage of pseudorandom function], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2012, No. 12 (137), pp. 218-224.
8. *Kalmykov I.A., Dagaeva O.I.* Primenenie sistemy ostatochnykh klassov dlya formirova-niya psevdosluchaynoy funktsii povyshennoy effektivnosti [Application of the system of residual classes for the formation of a pseudo-random function with increased efficiency], *Vestnik Severo-Kavkazskogo federal'nogo universiteta* [Bulletin of the North Caucasian Federal University], 2012, No. 3 (32), pp. 26-31.
9. *Camenisch J., Gross T., & Sommer D.* Assertion message signatures. Patent US 8 341 416 B2. 2012. December 25.
10. *Agbedemnab P.A. and Bankas E.K.* A Novel RNS Overflow Detection and Correction Algorithm for the Moduli Set 2^n-1, 2^n, 2^n+1, *International Journal of Computer Applications (0975 – 8887)*. January 2015, Vol. 110, No. 16, pp. 30-34.
11. *Chu J., Benaissa M.* Error detecting AES using polynomial residue number system, *Microprocessor and Microsystems*, 2013, No. 37, pp. 228-234.
12. *Kalmykov I.A., Pashintsev V.P., Vel'ts O.V., Kalmykov M.I.* Metody zashchity peredavae-moy informatsii dlya sistem udalennogo kontrolya i upravleniya vysokotekhnologicheskimi ob"ektami [Methods of protection of the transmitted information systems for remote monitoring and control of technological objects], *Vestnik Severo-Kavkazskogo federal'nogo universiteta* [Bulletin of the North Caucasian Federal University], 2014, No. 4 (43), pp.38-43.
13. *Kalmykov I.A., Sarkisov A.B., Makarova A.V., Kalmykov M.I.* Rasshirenie metodov zashchity sistem elektronnoy kommertsii na osnove modulyarnykh algebraicheskikh skhem [Enhanced protection methods of electronic commerce on the basis of modular algebraic scheme], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 2 (151), pp. 218-225.
14. *Kalmykov I.A., Dagaeva O.I., Naumenko D.O., Vel'ts O.V.* Sistemnyy podkhod k primene-niyu psevdosluchaynykh funktsiy v sistemakh zashchity informatsii [A systematic approach to the use of pseudo-random functions in the systems of information protection], *Vestnik Severo-Kavkazskogo federal'nogo universiteta* [Bulletin of the North Caucasian Federal University], 2012, No. 3 (32), pp. 26-34.
15. *Wang Q.* Compact k-spendable E-cash with Anonymity Control Based Offline TTP, *International Journal of Innovative Computing, Information and Control*, 2011, No. 7 (1), pp. 459-469.
16. *Kalmykov I.A., Kikhtenko O.A., Baril'skaya A.V., Dagaeva O.I.* Kriptograficheskaya sis-tema na baze nepozitsionnykh polinomial'nykh algebraicheskikh struktur [A cryptographic system based on non-polynomial algebraic structures], *Vestnik Severo-Kavkazskogo federal'nogo universiteta* [Bulletin of the North Caucasian Federal University], 2010, No. 2, pp. 51-57.
17. *Kalmykov I.A., Chipiga A.F., Kikhtenko O.A., Baril'skaya A.V.* Kriptograficheskaya zashchita dannykh v informatsionnykh tekhnologiyakh na baze nepozitsionnykh polinomial'nykh sistem [Cryptographic protection of data in information technology on base nepozicionnyh polynomial systems], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2009, No. 11 (100), pp. 210-220.
18. *Kalmykov I.A., Chipiga A.A.* Algoritm obespecheniya informatsionnoy skrytnosti dlya adaptivnykh sredst peredachi informatsii [Algorithm software information of stealth technology, adaptive means of transmitting information], *Infokommunikatsionnye tekhnologii* [Infocommunication Technologies], 2007, Vol. 5, No. 3, pp. 159-162.
19. *Kalmykov I.A., Kalmykov M.I.* Strukturnaya organizatsiya parallel'nogo spetsprotsessora tsifrovoy obrabotki signalov, ispol'zuyushchego modulyarnye kody [Structural organization of parallel special processor for digital signal processing using modular codes], *Teoriya i tekhnika radiosvyazi* [Theory and Technique of Radio Communication], 2014, No. 2, pp. 60-66.

20. *Berezhnoy V.V., Kalmykov, I.A. Chervyakov N.I., Shchelkunova Yu.O., Shilov A.A.* Neyrosetevaya realizatsiya v polinomial'noy sisteme klassov vychetov operatsiy TsOS povyshennoy razryadnosti [Neural implementation of a polynomial system classes deductions DSP operations increased bit depth], *Neyrokomp'yutery: razrabotka, primenenie* [Neurocomputers: development, application], 2004, No. 5-6, pp. 94.
21. *Kalmykov I.A., Rezen'kov D.N., Gordenko D.V., Sarkisov A.B.* Metody i algoritmy rekonfiguratsii nepozitsionnykh vychislitel'nykh struktur dlya obespecheniya otkazoustoychivosti spetsprotsessorov [Methods and algorithms for reconfiguration of non-computational structures for fault tolerance special processor]. Stavropol': Fabula, 2014, 180 p.
22. *Barsagaev A.A, Kalmykov M.I.* Algoritmy obnaruzheniya i korrektsii oshibok v modulyarnykh polinomial'nykh kodakh [Algorithms for detection and correction of errors in modular polynomial codes], *Mezhdunarodnyy zhurnal eksperimental'nogo obrazovaniya* [International journal of experimental education], 2014, No. 3-1, pp. 103-107.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Калмыков Игорь Анатольевич – Институт информационных технологий и телекоммуникаций Северо-Кавказского федерального университета, г. Ставрополь; e-mail: kia762@yandex.ru; 355040, г. Ставрополь, ул. Шпаковская, 92, кор. 1, кв. 28; тел.: 89034163533; кафедра информационной безопасности автоматизированных систем; д.т.н.; профессор.

Гиш Татьяна Александровна – e-mail: velts-yatsenco@yandex.ru; 355013, г. Ставрополь, ул. Чехова, 33, кв. 66; тел.: 88652944241; кафедра информационной безопасности автоматизированных систем; аспирант.

Науменко Даниила Олегович – e-mail: dante603@gmail.com; 355040, г. Ставрополь, ул. Семашко, 8, кв. 23; тел.: 89197362888; кафедра информационной безопасности автоматизированных систем; аспирант.

Калмыков Максим Игоревич – e-mail: kmi762@yandex.ru; 355040, г. Ставрополь, пр. Кулакова, 33, кв. 56; тел.: 88652956546; кафедра информационной безопасности автоматизированных систем; аспирант.

Дунин Андрей Валерьевич – e-mail: dav_26rus@mail.ru; 355007 г. Ставрополь, ул. Бурмистрова, 95; тел.: 89624465766; кафедра информационной безопасности автоматизированных систем; аспирант.

Kalmykov Igor Anatolyevich – Institute of Information Technologies and Telecommunications, North-Caucasus Federal University, Stavropol; e-mail: kia762@yandex.ru; 92, Shpakovskaya street, build. 1, ap. 28, Stavropol, 355000, Russia; phone: +79034163533; the department of information security of automated systems; dr. of eng. sc.; professor.

Gish Oksana Vladimirovna – e-mail: velts-yatsenco@yandex.ru; 33, Chehova street, ap. 66, Stavropol, 355000, Russia; phone: +78652944241; the department of information security of automated systems; postgraduate student.

Naumenko Daniil Olegovich – e-mail: dante603@gmail.com; 8, Semashko street, ap. 23, Stavropol, 355000, Russia; phone: +79197362888; the department of information security of automated systems; postgraduate student.

Kalmykov Maksim Igorevich – e-mail: kmi762@yandex.ru; 33, Kulakov av., ap. 56, Stavropol, 355040, Russia; phone: +79064710242; the department of information security of automated systems; postgraduate student.

Dunin Andrey Valeryevich – e-mail: dav_26rus@mail.ru; 95, Burmistrova street, Stavropol, 355007, Russia; phone: +79624465766; the department of information security of automated systems; postgraduate student.