УДК 004.052.2

МОДИФИКАЦИЯ МЕТОДА АУТЕНТИФИКАЦИИ НИЗКООРБИТАЛЬНЫХ СПУТНИКОВ НА ОСНОВЕ КОДОВ ПОЛИНОМИАЛЬНОЙ СИСТЕМЫ КЛАССОВ ВЫЧЕТОВ

Чистоусов Н.К., Калмыков И.А., Духовный Д.В., Калмыкова Н.И., Емельянов Е.А.
ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru

Современные глобальные проекты по освоению территорий Российской Федерации, расположенных за полярным кругом, привели к новому витку развития низкоорбитальных систем спутниковой связи (НССС). Так как высота орбиты НССС не превышает 1500 км, то спутник находится в зоне видимости приемника от 10 до 20 мин. Поэтому для обеспечения постоянной и достоверной связи с абонентами группировка НССС должна содержать от 40 до 66 космических аппаратов. Повышенный интерес к месторождениям полезных ископаемых, расположенным на шельфе Северного Ледовитого океана, приведет к увеличению числа группировок НССС. В результате этого у спутника-нарушителя появится возможность навязать ретрансляционную помеху, которая представляет собой перехваченную ранее и задержанную команду управления. Предотвратить такое деструктивное воздействие возможно путем повышения имитостойкости НССС за счет использования системы опознавания спутника. В основе работы данной системы предлагается использовать протоколы аутентификации с нулевым разглашением знаний. Однако они имеют недостаток – значительные временные затраты на опознавание из-за того, что при вычислениях используются большие простые числа. Сокращение времени опознавания спутника позволит уменьшить время, которое использует злоумышленник, чтобы подобрать правильный сигнал ответчика. Для решения данной проблемы в статье предлагается использовать коды полиномиальной системы классов вычетов (ПСКВ). Цель статьи – сократить время опознавания спутника за счет использования ПСКВ, в которых вычисления производятся параллельно и независимо по основаниям кода.

Ключевые слова: система опознавания спутника, протокол аутентификации на основе доказательства с нулевым разглашением, коды полиномиальной системы классов вычетов

MODIFICATION OF THE AUTHENTICATION METHOD FOR LOW-ORBIT SATELLITES BASED ON THE CODES OF THE POLYNOMIAL RESIDUE NUMBER SYSTEM

Chistousov N.K., Kalmykov I.A., Dukhovnyy D.V., Kalmykova N.I., Emelyanov E.A.
North-Caucasian Federal University, Stavropol, e-mail: kia762@yandex.ru

Modern global projects for the development of the territories of the Russian Federation located beyond the Arctic Circle have led to a new round of development of low-orbit satellite communication systems (LowSCS). Since the altitude of the LowSCS orbit does not exceed 1500 km, the satellite is in the range of visibility of the receiver from 10 to 20 minutes. Therefore, in order to ensure constant and reliable communication with subscribers, the LowSCS grouping should contain from 40 to 66 spacecraft. Increased interest in mineral deposits located on the shelf of the Arctic Ocean will lead to an increase in the number of groups of LowSCS. As a result, the intruder satellite will have the opportunity to impose a relay interference, which is a previously intercepted and delayed control command. It is possible to prevent such a destructive impact by increasing the imitability of the LowSCS through the use of a satellite identification system. At the heart of the work of this system, it is proposed to use authentication protocols with zero knowledge disclosure. However, they have a disadvantage – significant time spent on identification due to the fact that large prime numbers are used in calculations. Reducing the time of satellite identification will reduce the time that an attacker uses to pick up the correct responder signal. To solve this problem, the article proposes to use the codes of the polynomial residue number system (PRNS). The purpose of the article is to reduce the time of satellite identification through the use of PRNS, in which calculations are performed in parallel and independently on the basis of the code.

Keywords: satellite identification system, protocol with authentication zero-knowledge proof knowledge, polynomial residue number system codes

Повышенный интерес компаний к освоению месторождений полезных ископаемых, находящихся за полярным кругом, связан с тем, что, по прогнозам ученых, на шельфе Северного Ледовитого океана сосредоточено более 20% мировых запасов нефти и газа [1]. Для организации эффективной добычи и транспортировки углеводородов компании используют автоматизированные системы дистанционного мониторинга, контроля и управления (АСДМКУ). При этом для организации постоянного и достоверного обмена данными между оперативным центром и необслуживаемыми объектами управления (НОУ) используются низкоорбитальные системы спутниковой связи (НССС), имеющие в своем составе не менее 40 космических аппаратов (КА). По мере освоения месторождений будет увеличиваться число группировок НССС. В результате этого в зону видимости приемника, расположенного на НОУ, могут попасть сразу несколько КА. В этом случае спутник-нарушитель получит возможность

навязать ретрансляционную помеху, которая представляет собой переданную ранее команду управления. Предотвратить такое деструктивное воздействие возможно путем повышения имитостойкости НССС за счет использования системы опознавания КА.

В основе работы систем опознавания КА предлагается использовать протоколы аутентификации с нулевым разглашением знаний [2]. Так как данные методы аутентификации используют большие простые числа, то они имеют недостаток – значительные временные затраты на опознавание. При этом чем больше времени на опознавание КА, тем больше вероятность того, что нарушитель сможет подобрать правильный сигнал ответчика. Сократить время вычисления за счет уменьшения разрядности простых чисел нельзя, так как это снижает стойкость протокола аутентификации. Решить эту проблему можно за счет применения кодов полиномиальной системы классов вычетов (ПСКВ). Цель статьи – сократить время опознавания КА за счет ПСКВ, так как в этих кодах вычисления осуществляются с остатками и производятся параллельно и независимо по основаниям.

Материалы и методы исследования

При построении системы опознавания, которая состоит из запросчика и ответчика, часто применяются методы аутентификации, использующие системы шифрования. Данные системы позволяют обеспечить высокую криптостойкость запросно-ответной системы к подбору правильного сигнала ответчика. При этом, как правило, используются симметричные системы шифрования. В этом случае сигнал запросчика (З) $M_З$ представляет собой зашифрованное с помощью секретного ключа К случайное число $R_З$. Ответчик расшифровывает сигнал запросчика и получает число $R_З$. Затем он, используя секретный ключ К, генерирует зашифрованный сигнал ответчика (О) $M_О$, который поступает запросчику. Последний расшифровывает его и получает $R_З - 1$. Данный процесс опознавания можно представить в виде

$$\begin{aligned} &З \rightarrow О : M_З = E_К(R_З), \\ &О : R_З = D_К(M_З), \\ &О \rightarrow: M_О = E_К(R_З - 1), \\ &З : R_З - 1 = D_К(M_О). \end{aligned} \qquad (1)$$

Выбор симметричных систем шифрования для выполнения протокола (1) определяется тем, что они обеспечивают минимальные временные затраты на аутентификацию. В работе [3] показано, что максимальная скорость симметричного шифрования в системе на кристалле ATL186 достигает значения 400 Мбит/с. Однако при использовании симметричных шифров в системах опознавания возникает проблема, связанная с доставкой секретных ключей запросчику и ответчику. Особенно она актуальна для систем опознавания космических аппаратов, которые несколько лет находятся на орбите. Если в процессе передачи запросчику или ответчику злоумышленник сможет перехватить секретный ключ, то он легко подделает сигнал ответчика. В результате этого снизится имитостойкость НССС и спутник-нарушитель получит доступ к каналу связи.

Обеспечить высокую имитостойкость НССС позволяют методы аутентификации, которые используют протоколы с нулевым разглашением знаний. Данные протоколы имеют высокую вычислительную сложность, благодаря которой обеспечивается низкая вероятность подбора правильного ответа без использования шифрования [4]. Первыми протоколами аутентификации были протоколы Фиат – Шамира и Фейге – Фиат – Шамира. Для обеспечения высокой криптостойкости для протокола Фиат – Шамира надо было реализовать от 20 до 40 раундов вычислений, а для протокола Фейге – Фиат – Шамира – от 4 до 8 раундов. Для снижения временных затрат на аутентификацию были разработаны протоколы Шнорра, Гиллу – Кискатра. Дальнейшее снижение времени на аутентификацию обеспечил протокол, приведенный в работе [5]. Данный результат был достигнут за счет уменьшения числа операций на этапе аутентификации претендента.

Несмотря на то, что данные протоколы имеют только один раунд аутентификации, она не обеспечивают максимальную скорость аутентификации, так как все вычисления производятся по большому модулю. Для снижения временных затрат на выполнение аутентификации в работе [6] предложено использовать коды системы остаточных классов вычетов (СОК). В данных кодах вычисления производятся по основаниям, в качестве которых использовались простые числа.

Дальнейшее повышение имитостойкости НССС возможно за счет применения кодов ПСКВ, которые, обладая скоростью проводимых вычислений, сравнимой с кодами СОК, способны генерировать большее количества ответных сигналов благодаря использованию многочленов, имеющих одинаковую степень. В этих кодах ПСКВ целые числа представляются в полиномиальной форме. Затем полученные полино-

мы делятся на неприводимые многочлены $m_i(x)$, где i = 1, 2, … n, которые являются основаниями ПСКВ. В результате получается кортеж остатков $C_i(x) \equiv C(x) \bmod m_i(x)$, где i = 1, 2, … n

$$C(x) = (C_1(x), C_2(x), ..., C_n),$$

Принципы построения и выполнение модульных операций в кодах ПСКВ приведены в работе [7]. Для модульных операций справедливо

$$C(x) \oplus A(x) = ((C_1(x) \oplus A_1(x)) \bmod m_1(x), ..., (C_n(x) \oplus A_n(x)) \bmod m_n(x)), \quad (2)$$

$$C(x)A(x) = ((C_1(x)A_1(x)) \bmod m_1(x), ..., (C_n(x)A_n(x)) \bmod m_n(x)), \quad (3)$$

где $A_i(x) \equiv A(x) \bmod m_i(x)$; i = 1, 2, … n.

Количество разрешенных комбинаций кода ПСКВ задается рабочим диапазоном

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

Проведем модификацию метода аутентификации КА, представленного в [4]. Набор оснований осуществляется так, чтобы выполнялось условие

$$\log_2 \{W, Q, E\} < \deg M_n(x), \quad (5)$$

где W – секретный ключ КА; Q – случайное число; E – случайное число.

Число Q позволяет генерировать сеансовый ключ Q(j), где j – номер сеанса. Так как в процессе генерации Q(j) может произойти сбой, то операционный центр должен определить повторное использование Q(j). Для этого используется случайное число E, используемое для генерации параметра E(j), с помощью которого можно проверить повторное применение Q(j). В качестве порождающего элемента выбираем e(x) = x.

Предварительный этап протокола аутентификации в ПСКВ.

1. Ответчик вычисляет секретные параметры для j-го сеанса, где j = 1, 2, ….

$$O: Q(j) = x^{(W(j)+Q(j-1))^{-1}} \bmod S, \quad (6)$$

где S – большое простое число;
$\log_2 \{S\} < \deg M_n(x)$.

$$O: E(j) = x^{(W(j)+Q(j-1)+E(j-1))^{-1}} \bmod S. \quad (7)$$

2. Ответчик представляет секретные параметры в виде кода ПСКВ

$$O: W(j) = (W_1(j) \| W_2(j) \| ... \| W_n(j)),$$
$$O: Q(j) = (Q_1(j) \| Q_2(j) \| ... \| Q_n(j)), \quad (8)$$
$$O: E(j) = (E_1(j) \| E_2(j) \| ... \| E_n(j)),$$

где $\deg W_i = \deg m_i(x)$; $\deg Q_i(0) = \deg m_i(x)$; $\deg E_i(0) = \deg m_i(x)$.

3. Ответчик вычисляет «истинный» статус КА для j-го сеанса

$$O: \begin{cases} A_1^j(x) = x^{W_1(j)} x^{Q_1(j)} x^{E_1(j)} \bmod m_1(x), \\ \vdots \\ A_n^j(x) = x^{W_n(j)} x^{Q_n(j)} x^{E_n(j)} \bmod m_n(x). \end{cases} \quad (9)$$

4. Ответчик искажает секретные параметры с помощью случайных чисел таких, что

$$\{\Delta W_i(j), \Delta Q_i(j), \Delta E_i(j)\} < V_i = 2^{\deg m_i(x)} - 1. \quad (10)$$

Тогда «искаженные» параметры спутника имеют вид

$$O: \tilde{W}_i(j) = W_i(j) + \Delta W_i(j) \bmod V_i,$$
$$O: \tilde{Q}_i(j) = Q_i(j) + \Delta Q_i(j) \bmod V_i, \quad (11)$$
$$O: \tilde{E}_i(j) = E_i(j) + \Delta E_i(j) \bmod V_i.$$

5. Ответчик вычисляет «искаженный» статус КА для j-го сеанса:

$$O: \begin{cases} \tilde{A}_1^j(x) = x^{\tilde{W}_1(j)} x^{\tilde{Q}_1(j)} x^{\tilde{E}_1(j)} \bmod m_1(x), \\ \vdots \\ \tilde{A}_n^j(x) = x^{\tilde{W}_n(j)} x^{\tilde{Q}_n(j)} x^{\tilde{E}_n(j)} \bmod m_n(x). \end{cases} \quad (12)$$

Процесс аутентификации космического аппарата.

1. Запросчик передает случайное число B < S, представив его в коде ПСКВ

$$З: B(j) = x^{(B(j-1))^{-1}} \bmod S,$$
$$З \rightarrow O: B(j) = (B_1(j) \| B_2(j) \| ... \| B_n(j)). \quad (13)$$

2. Ответчик, получив сигнал запросчика, выполняет выражения

$$O: H_i^1(j) = \tilde{W}_i(j) - B_i(j) W_i(j) \bmod V_i,$$
$$O: H_i^2(j) = \tilde{Q}_i(j) - B_i(j) Q_i(j) \bmod V_i, \quad (14)$$
$$O: H_i^3(j) = \tilde{E}_i(j) - B_i(j) E_i(j) \bmod V_i.$$

3. Ответчик передает свой сигнал запросчику

$$O \to З: \left\{A_i^j(x),\ \tilde{A}_i^j(x),\ H_i^1(j),\ H_i^2(j),\ H_i^3(j)\right\}. \quad (15)$$

4. Запросчик получает сигнал ответчика и проверяет его

$$O: \begin{cases} P_1^j(x) = \left(\left(A_1^j(x)\right)^{B_1(j)} x^{H_1^1(j)} x^{H_1^2(j)} x^{H_1^3(j)}\right) \bmod m_1(x), \\ \vdots \\ P_n^j(x) = \left(\left(A_n^j(x)\right)^{B_n(j)} x^{H_n^1(j)} x^{H_n^2(j)} x^{H_n^3(j)}\right) \bmod m_n(x). \end{cases} \quad (16)$$

6. Запросчик принимает решение «спутник свой», если выполняется

$$Y_i^j(x) = \left|\left(C_i^j(x)\right)^{d_i^j} g(x)^{r_i^1} g(x)^{r_i^2} g(x)^{r_i^3}\right|_{p_i(x)}^{+}. \quad (17)$$

Спутнику присвоят статус «свой», если справедливо

$$\left\{P_1^j(x) = \tilde{A}_1^j(x), ..., P_n^j(x) = \tilde{A}_n^j(x)\right\}. \quad (18)$$

Результаты исследования и их обсуждение

Выбираем секретные параметры из условия $\log_2\{W, Q, E\} < 15$ бит. Тогда ПСКВ содержит $p_1(x) = x^5 + x^4 + x^3 + x + 1$, $p_2(x) = x^5 + x^4 + x^3 + x^2 + 1$, $p_3(x) = x^5 + x^3 + x^2 + x + 1$ Рабочий диапазон $M_3(x) = x^{15} + x^{11} + x^{10} + x^2 + 1$. Ответчик получил секретные параметры в ПСКВ:

$$W(j) = 25841 = W_1(j) \| W_2(j) \| W_3(j) = 11001 \| 00111 \| 10001 = 25_{10} \| 7_{10} \| 17_{10}.$$

$$Q(j) = 10872 = Q_1(j) \| Q_2(j) \| Q_3(j) = 01010 \| 10011 \| 11000 = 10_{10} \| 19_{10} \| 24_{10}.$$

$$E(j) = 4450 = E_1(j) \| E_2(j) \| E_3(j) = 00100 \| 01011 \| 00010 = 4_{10} \| 11_{10} \| 2_{10}.$$

Ответчик вычисляет «истинный» статус КА для j-го сеанса

$$O: \begin{cases} A_1^j(x) = x^{25} \cdot x^{10} \cdot x^4 \bmod x^5 + x^4 + x^3 + x + 1 = \left|x^8\right|_{x^5+x^4+x^3+x+1}^{+} = x^3 + x^2 + x + 1 = 15_{10}. \\ A_2^j(x) = x^7 \cdot x^{19} \cdot x^{11} \bmod x^5 + x^4 + x^3 + x^2 + 1 = \left|x^6\right|_{x^5+x^4+x^3+x^2+1}^{+} = x^2 + x + 1 = 7_{10}. \\ A_3^j(x) = x^{17} \cdot x^{24} \cdot x^2 \bmod x^5 + x^3 + x^2 + x + 1 = \left|x^{12}\right|_{x^5+x^3+x^4+x+1}^{+} = x + 1 = 3_{10}. \end{cases}$$

Ответчик искажает секретные параметры с помощью случайных чисел таких, что

$$\Delta W(j) = (2, ,3, 15),\ \Delta Q(j) = (3, 16, 10)\ \Delta E_i(j) = (20, 12, 17).$$

Тогда «искаженные» параметры спутник имеют вид

$$O: \tilde{W}_1(j) = 25 + 2 \bmod 31 = 27,\ \tilde{W}_2(j) = 7 + 3 \bmod 31 = 10,\ \tilde{W}_3(j) = 17 + 15 \bmod 31 = 1,$$

$$O: \tilde{Q}_1(j) = 10 + 3 \bmod 31 = 13\ ,\tilde{Q}_2(j) = 19 + 16 \bmod 31 = 4\ ,\tilde{Q}_3(j) = 24 + 10 \bmod 31 = 3,$$

$$O: \tilde{E}_1(j) = 4 + 20 \bmod 31 = 24, \tilde{E}_2(j) = 11 + 12 \bmod 31 = 23, \tilde{E}_1(j) = 2 + 17 \bmod 31 = 19.$$

Ответчик вычисляет «искаженный» статус КА для j-го сеанса

$$O: \begin{cases} \tilde{A}_1^j(x) = x^{27} \cdot x^{13} \cdot x^{24} \bmod x^5 + x^4 + x^3 + x + 1 = \left|x^2\right|_{x^5+x^4+x^3+x+1}^{+} = x^2 = 4_{10}. \\ \tilde{A}_2^j(x) = x^{10} \cdot x^4 \cdot x^{23} \bmod x^5 + x^4 + x^3 + x^2 + 1 = \left|x^6\right|_{x^5+x^4+x^3+x^2+1}^{+} = x^2 + x + 1 = 7_{10}. \\ \tilde{A}_3^j(x) = x^1 \cdot x^3 \cdot x^{19} \bmod x^5 + x^3 + x^2 + x + 1 = \left|x^{19}\right|_{x^5+x^3+x^4+x+1}^{+} = x^4 + x^3 + x = 26_{10}. \end{cases}$$

Процесс аутентификации КА. Запросчик передает ответчику случайное число

$$З \rightarrow О: B(j) = B_1(j) \,||\, B_2(j) \,||\, B_3(j) = 00101 \,||\, 01010 \,||\, 00111 = 5 \,||\, 10 \,||\, 7.$$

Ответчик, получив сигнал запросчика, выполняет выражения

$$O: H_1^1(j) = \left|27 - 5 \cdot 25\right|_{31}^{+} = 26,\ H_2^1(j) = \left|13 - 5 \cdot 10\right|_{31}^{+} = 25,\ H_3^1(j) = \left|24 - 5 \cdot 4\right|_{31}^{+} = 4,$$

$$O: H_1^2(j) = \left|10 - 10 \cdot 7\right|_{31}^{+} = 2,\ H_2^2(j) = \left|5 - 10 \cdot 19\right|_{31}^{+} = 1,\ H_3^2(j) = \left|23 - 10 \cdot 11\right|_{31}^{+} = 6,$$

$$O: H_1^3(j) = \left|1 - 7 \cdot 17\right|_{31}^{+} = 6,\ H_2^3(j) = \left|3 - 7 \cdot 24\right|_{31}^{+} = 21,\ H_3^3(j) = \left|19 - 7 \cdot 2\right|_{31}^{+} = 5.$$

Ответчик передает сигнал О → З: {(15, 7, 3)(4, 7, 26)(26, 25, 4)(2, 1, 6)(6, 21, 5)}. Запросчик, получает сигнал ответчика и проверяет его

$$O: \begin{cases} P_1^j(x) = \left(x^3 + x^2 + x + 1\right)^5 x^{26} \cdot x^{25} \cdot x^4 \bmod x^5 + x^4 + x^3 + x + 1 = x^2 = \tilde{A}_1^j(x), \\ P_2^j(x) = \left(x^2 + x + 1\right)^{10} x^2 \cdot x^1 \cdot x^6 \bmod x^5 + x^4 + x^3 + x^2 + 1 = x^2 + x + 1 = \tilde{A}_2^j(x), \\ P_3^j(x) = \left(x + 1\right)^7 x^6 \cdot x^{21} \cdot x^5 \bmod x^5 + x^3 + x^2 + x + 1 = x^4 + x^3 + x = \tilde{A}_3^j(x). \end{cases}$$

Запросчик принимает решение «спутник свой» и предоставляет сеанс связи.

На основе модифицированного метода аутентификации была разработана структурная модель системы опознавания КА, которая была реализована на FPGA Xilinx Artix-7 (xc7s6ftgb196-1). Тестирование велось на платформе Vivado HLS 2019.1. Для одномодульного метода аутентификации выбрано S = 11337409. В модифицированном методе были использованы пять полиномов пятой степени. Операции возведения в степень по модулю были выполнены с помощью алгоритма Монтгомери. Исследования показали, что при использовании одномодульного протокола аутентификации для опознавания спутника необходимо T_o = 5936 нс. В данном показателе представлено время на получение истинного и «искаженного» статуса КА, вычисление ответов на вопрос запросчика и проведение проверки этих ответов. Временные затраты на получение параметров Q(j), E(j) и вопроса запросчика B(j) не учитывались. Исследование модифицированного метода аутентификации на основе ПСКВ показало, что временные затраты на опознавание равны $T_{ПСКВ}$ = 3238 нс. Таким образом, использование кодов ПСКВ позволило сократить время опознавания спутника в 1,83 раза за счет выполнения параллельных вычислений с малоразрядными операндами. Таким образом, сокращение времени опознавания КА повысит имитостойкость НССС за счет уменьшения вероятности подбора злоумышленником правильного сигнала ответчика.

Заключение

В статье проведена модификация метода аутентификации для низкоорбитальных спутников на основе кодов ПСКВ. Использование данных кодов сокращает временные затраты на опознавание КА за счет параллельного выполнения вычислений с малоразрядными остатками. Для оценки эффективности модифицированного метода аутентификации была разработана структурная модель системы опознавания КА, которая была реализована на FPGA Xilinx Artix-7. Исследования показали, что при использовании одномодульного метода аутентификации для опознавания КА потребуется T_o = 5936 нс, а при использовании модифицированного метода – $T_{ПСКВ}$ = 3238 нс. Таким образом, использование кодов ПСКВ позволило сократить время опознавания спутника в 1,83 раза за счет выполнения параллельных вычислений с малоразрядными операндами.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-37-90009.

Список литературы

1. Андреева Е.В., Исаулова К.Я. Перспективы развития СМП // Деловой журнал «Neftegaz.RU». 2021. № 6. С. 30–37.

2. Rezenkov R.N., Pashintsev V.P., Zhuk P.A., Kalmykov M.I. Application of spoof resistant authentication protocol of spacecraft in low earth orbit systems of satellite communication. International Journal of Mechanical Engineering and Technology (IJMET). 2018. Vol 9. No. 5. P. 958–965.

3. Архипкин В.А. ЗАО «СБТ» на пути к импортозамещению: система на кристаллах ATL186 для современных систем и средств связи // Связь в Вооруженных Силах Российской Федерации. 2015. С. 202–203.

4. Запечников С.В., Казарин О.В. Криптографические методы защиты информации. М.: Издательство Юрайт, 2019. 309 с.

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

6. Чистоусов Н.К., Чипига А.Ф. Разработка протоколов аутентификации низкоорбитальных космических аппаратов на основе параллельных кодов систем остаточных классов // Инженерный вестник Дона. 2021. № 4. URL: http://www.ivdon.ru/ru/magazine/archive/n4y2021/6912 (дата обращения 02.02.2022).

7. Ananda Mohan Residue Number Systems. Theory and Applications. Springer International Publishing Switzerland, 2016. 351 p.