Агібалов О. П., Поляков М. О.

ТРАНСЛЯТОР ПАРАМЕТРІВ МОДЕЛІ КІНЦЕВОГО АВТОМАТА ІЗ СЕРЕДОВИЩА MATLAB У ДОДАТОК ЛЮДИНО-МАШИННОГО ІНТЕРФЕЙСУ

Запропоновано технологію та засоби автоматичного переносу параметрів моделі кінцевого автомату з додатку Matlab до додатку людино-машинного інтерфейсу. Розглянуто приклад застосування технології до моделі електричного апарата.

Ключові слова: stateflow, кінцевий автомат, DDE-діалог, людино-машинний інтерфейс, тег.

Agibalov A. P., Polyakov M. A.

TRANSLATOR OF FINITE STATE MACHINE MODEL PARAMETERS FROM MATLAB ENVIRONMENT INTO HUMAN-MACHINE INTERFACE APPLICATION

Technology and means for automatic translation of FSM model parameters from Matlab application to human-machine interface application is proposed. The example of technology application to the electric apparatus model is described.

Key words: stateflow, finite-state machine, DDE-dialog, human-machine interface, tag.

УДК 004.056.53:004.75

Андрущенко Д. М.[1], Варава М. Ю.[2], Неласа Г. В.[3]

[1]Молодший науковий співробітник Запорізького національного технічного університету
[2]Провідний спеціаліст з інформаційних технологій КБ Приватбанк
[3]Канд. техн. наук, доцент Запорізького національного технічного університету

РОЗПАРАЛЕЛЮВАННЯ ρ - І λ - МЕТОДІВ ПОЛЛАРДА РОЗВ'ЯЗАННЯ ЗАДАЧІ ДИСКРЕТНОГО ЛОГАРИФМУВАННЯ

Проведено аналіз ефективності розпаралелювання ρ - і λ -методів Полларда при вирішенні задачі дискретного логарифмування. Наводиться теоретична оцінка часу виконання завдання на паралельній системі. Проведено порівняння результатів практичних і теоретичних розрахунків. Зроблені заміри часу виконання розпаралелених методів.

Ключові слова: методи Полларда, дискретний логарифм, розпаралелювання, складність криптоалгоритма, оцінка складності.

ВСТУП

При створенні систем захисту інформації широко застосовуються асиметричні алгоритми. Надійність таких систем основана на трудомісткості виконання одного з наступних типів зворотних перетворень: розкладання великих чисел на прості множники; обчислення дискретного логарифму; обчислення коренів алгебраїчних рівнянь [1, 2]. Однак розвиток методів прискорених обчислень, в тому числі застосування багатопроцесорних систем паралельних рішень, викликає небезпеку зниження ступеню захисту криптосистем. Тому для оцінки надійності систем захисту та їх вдосконалення необхідно дослідження методів паралельних рішень для проведення названих перетворень.

ПОСТАНОВКА ЗАДАЧІ

Одними з найбільш розповсюджених асиметричних криптосистем є ті, що створені на базі еліптичних кривих $y^2 = x^3 + ax + b \bmod p$ над простим полем $GF(p)$. Якщо P є базовою точкою адитивної групи точок еліптичної кривої простого порядку n, точка Q належить заданій групі точок еліптичної кривої, то злом криптографічної системи полягає у розв'язанні рівняння $m \cdot P = Q$ відносно m, де $1 < m < n-1$ (адитивний аналог задачі дискретного логарифмування).

Надійність систем захисту інформації, злом яких оснований на розв'язанні задачі дискретного логарифмування залежить від величини n. Однак, збільшення n, окрім підвищення надійності, призводить до збільшення часу роботи криптографічних алгоритмів. Тому для побудови ефективних алгоритмів необхідний компромісний варіант, що забезпечує достатню надійність захисту при прийнятному рівні модуля n з точки зору швидкості роботи алгоритму. Поява нових методів прискорення обчислень дискретного логарифму, одним з яких є розпаралелювання, викликає необхідність збільшення параметру n. Тому оцінка ступеня надійності криптографічних систем, дослідження можливості їх злому шляхом розпаралелювання процесу розв'язання задачі дискретного логарифмування є актуальною проблемою.

Відомі різні алгоритми послідовного вирішення цього завдання, в тому числі: великих-малих кроків, Поліга-Хеллмана, ρ-Полларда, λ-Полларда, Адлемана, index-calculus [1–3]. Більшість з них піддаються розпаралелюванню. У даній роботі для перевірки працездатності системи та оцінки ефективності даного підходу були розглянуті ρ-метод і λ-метод Полларда [2].

Метод ρ -Полларда. Ідея методу полягає в побудові послідовності точок Z_i еліптичної кривої

$$Z_i = A_i P + B_i Q, \qquad (1)$$

де $1 < A_i, B_i < n-1$,

яка забезпечує знаходження пари рівних точок Z_i і Z_j:

$$Z_i = Z_j, i \neq j. \quad (2)$$

У цьому випадку одержимо

$$A_i P + B_i Q = A_j P + B_j Q, \quad (3)$$

звідси

$$Q = \frac{A_j - A_i}{B_i - B_j} P. \quad (4)$$

Таким чином,

$$d = \frac{A_j - A_i}{B_i - B_j} (\mathrm{mod}\, n), \; B_i \neq B_j. \quad (5)$$

Для реалізації методу оберемо два випадкових числа A_0, $B_0 \in [0, n-1]$, так щоб одночасно A_0 і B_0 не були рівними нулю:

$$Z_0 = A_0 P + B_0 Q. \quad (6)$$

Розіб'ємо відрізок $(0, p)$ на три рівних множини S_1, S_2 й S_3 і обчислимо Z_{i+1} рекурентне за правилом

$$Z_{i+1} = \begin{cases} 2Z_i, & \text{якщо} \quad Z_i^x \in S_1; \\ Z_i + P, & \text{якщо} \quad Z_i^x \in S_2; \\ Z_i + Q, & \text{якщо} \quad Z_i^x \in S_3; \end{cases} \quad (7)$$

де Z_i^x визначає x-координату точки на еліптичній кривій.

Звідси

$$A_{i+1} = \begin{cases} 2A_i, & \text{якщо} \quad Z_i^x \in S_1; \\ A_i + 1, & \text{якщо} \quad Z_i^x \in S_2; \\ A_i, & \text{якщо} \quad Z_i^x \in S_3; \end{cases} \quad (8)$$

$$B_{i+1} = \begin{cases} 2B_i, & \text{якщо} \quad Z_i^x \in S_1; \\ B_i, & \text{якщо} \quad Z_i^x \in S_2; \\ B_i + 1, & \text{якщо} \quad Z_i^x \in S_3. \end{cases} \quad (9)$$

Метод ρ-Полларда проілюстровано на рис. 1.

Метод λ-Полларда. Очевидно, колізію точок можна одержати й іншим шляхом, рухаючись із двох (або більше) різних точок Z_k й Z_l до збігу $Z_{k+s} = Z_{l+t}$. Ця ситуація відображена на рис. 2. Даний метод одержання колізії називається λ-методом Полларда, походження назви якого зрозуміло з рисунка.

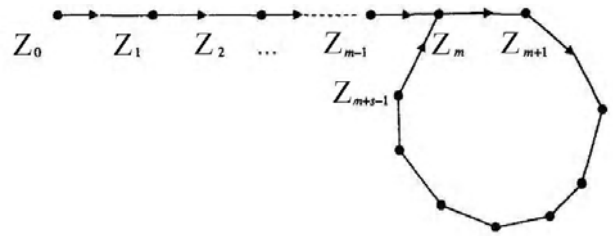

Рис. 1. ρ-метод Полларда

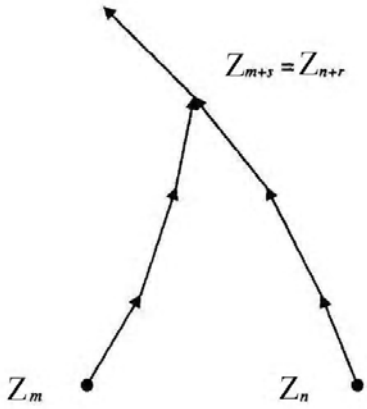

Рис. 2. λ-метод Полларда

Цей метод також може бути основою для розпаралелювання задачі обчислювання дискретного логарифму за допомогою r комп'ютерів, що може в r раз прискорити розв'язання задачі дискретного логарифмування.

РОЗПАРАЛЕЛЮВАННЯ МЕТОДІВ ПОЛЛАРДА

Алгоритм ρ-Полларда при великих значеннях n стає неефективним. Він може бути поліпшений, якщо всю множину точок еліптичної кривої, включаючи точку нескінченності, розбивати на $r > 3$ множин, які не перетинаються. У цьому випадку послідовність Z_i задається у вигляді:

$$Z_{i+1} = \begin{cases} (Z_i + c_1 G + d_1 Q), & \text{якщо} \quad Z_i \in S_1; \\ (Z_i + c_2 G + d_2 Q), & \text{якщо} \quad Z_i \in S_2; \\ \ldots\ldots\ldots\ldots\ldots & \ldots\ldots \quad \ldots\ldots\ldots \\ (Z_i + c_r G + d_r Q), & \text{якщо} \quad Z_i \in S_r; \end{cases} \quad (10)$$

де c_v, d_v – випадкові цілі числа з інтервалу $[0, n-1]$.

При використанні ітераційних формул виду (10) можна зменшити складність (вартість часу) процедури криптоаналізу. Крім того, застосування цього підходу дозволяє ефективно розпаралелювати процес знаходження коефіцієнтів c_v, d_v принаймні на r процесів.

Якщо числа c_v й d_v вибирати таким чином, щоб перетинання значень Z_i в областях не було, то й кожну

область можна розбити на необхідне число підобластей, що дозволяє розпаралелювати задачу на необхідну кількість незалежних процесів. Результати роботи кожного із процесів у вигляді трійок чисел $<Z_i, c_i, d_i>$ заносяться в загальну базу даних. Центральний процесор здійснює паралельний пошук значень $Z_i = Z_j$, $i \neq j$, і після цього можливе обчислення значення m.

Ілюстрацію розпаралелених ρ - і λ -методів Полларда наведено на рис. 3 та рис. 4.

Однією з головних характеристик паралельних систем є прискорення R паралельної системи, що визначається формулою: $R = T_1 / T_r$, де T_1 – час розв'язання задачі на однопроцесорній системі, а T_r – час розв'язання тієї ж задачі на r - процесорній системі. Нехай $W = W_{ск} + W_{пр}$, де W – загальне число операцій, $W_{пр}$ – число операцій, які можна виконувати паралельно, а $W_{ск}$ – число скалярних (нерозпаралелених) операцій. Позначимо також через t час виконання однієї операції. Тоді одержуємо оцінку для прискорення R

$$R = \frac{W \cdot t}{(W_{ск} + \frac{W_{пр}}{r}) \cdot t} = \frac{1}{a + \frac{1-a}{r}} \underset{r \to \infty}{\longrightarrow} \frac{1}{a}, \qquad (11)$$

де $a = W_{ск} / W$.

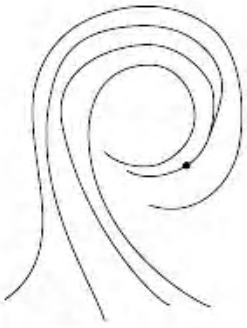

Рис. 3. Розпаралелений ρ -метод Полларда

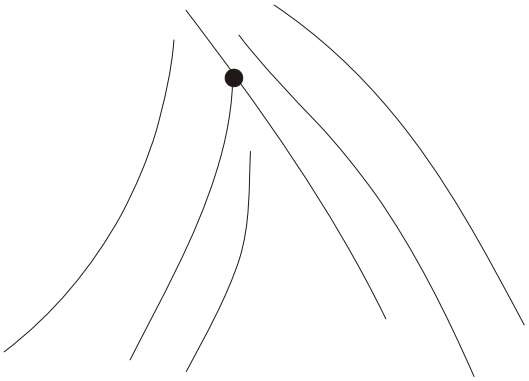

Рис. 4. Розпаралелений λ - метод Полларда

Таким чином, якщо 9/10 програми виконується паралельно, а 1/10 як і раніше послідовно, то більшого, ніж в 10 разів, прискорення одержати в принципі неможливо без втрат якості реалізації паралельної частини коду й кількості використаних процесів. Очевидно, що 10-кратне прискорення досягається тільки в тому випадку, коли час виконання паралельної частини дорівнює нулю.

Розпаралелювання ρ - і λ -методів Полларда дозволить проводити криптоаналіз протоколів не за рахунок підвищення продуктивності окремого комп'ютера, а завдяки масовому використанню паралельно підключених комп'ютерів у мережі.

Складність методу ρ -Полларда оцінюється як [4]:

$$I_\rho = \sqrt{\frac{\pi n}{4}}. \qquad (12)$$

Однією з переваг ρ -методу Полларда є те, що він допускає розпаралелювання на r незалежних процесів. У цьому випадку складність реалізації кожного із процесів можна оцінити як:

$$I_{\rho_1} = \frac{\sqrt{\frac{\pi n}{4}}}{r} = \sqrt{\frac{\pi n}{4r^2}}. \qquad (13)$$

ОСНОВНІ РЕЗУЛЬТАТИ

На рис. 5 зображена залежність часу криптоаналізу L від порядку криптосистеми n й числа розпаралелених процесів r для ρ -методу Полларда. Як видно із графіка, використання паралельного виконання алгоритму, криптоаналіз має сенс, коли число процесів не більше 17–19.

Складність методу λ -Полларда оцінюється як [4]

$$I_\lambda = 2\sqrt{n}, \qquad (14)$$

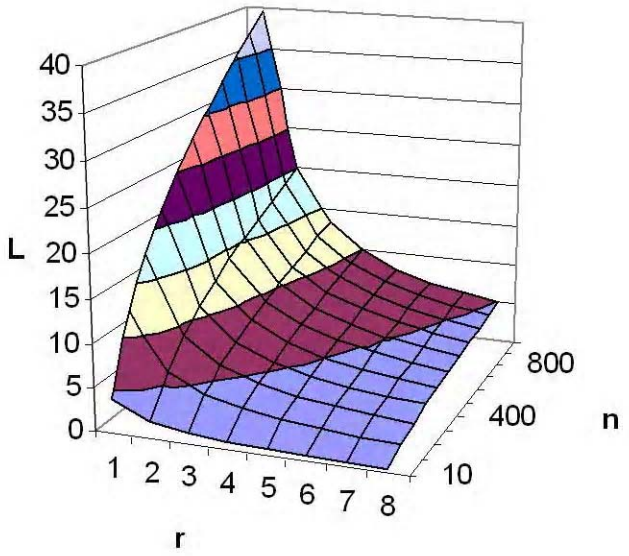

Рис. 5. Складність ρ -методу Полларда

а при розпаралелюванні

$$I_{\lambda_1} = \frac{2\sqrt{n}}{r}. \qquad (15)$$

На рис. 6 зображена залежність часу криптоаналізу від порядку криптосистеми й числа розпаралелених процесів для λ-методу Полларда. Як видно із графіка, λ-метод Полларда вимагає більше часу для обчислень, ніж ρ-метод Полларда. Отже, доцільно використовувати ρ-метод Полларда.

Проведемо порівняльний аналіз по складності названих методів. Для цього знайдемо відношення:

$$\frac{I_\lambda}{I_\rho} = \frac{2\sqrt{n}}{\sqrt{\frac{\pi n}{4}}} = \frac{4}{\sqrt{\pi}} \approx 2{,}26. \qquad (16)$$

З цього відношення випливає, що λ-метод Полларда більше, ніж в 2 рази складніший за метод ρ-Полларда.

ОЦІНКА ЧАСУ ВИКОНАННЯ РОЗПАРАЛЕЛЕНИХ ρ- І λ-МЕТОДІВ ПОЛЛАРДА

У ході виконання дослідження були зроблені заміри часу виконання розпаралелених ρ- і λ-методів Полларда. Програма була запущена на виконання по черзі на 4-х, на 5-х, на 6-х і на 7-х комп'ютерах. Результати тестування наведені в табл. 1 і на рис. 7.

Як видно з таблиці 1 й графіка на рис. 7, час виконання програми методом λ-Полларда в середньому більше, ніж час виконання аналогічної програми методом ρ-Полларда в 2 рази.

Були проведені виміри часу виконання програми методом ρ-Полларда з порядками базових точок $n=2^{64}$, 2^{73}, 2^{84}, 2^{96} на комп'ютерах AMD AtlonXP 1000+. Результати наведені в табл. 2 і на рис. 8. Час розв'язання задачі на одному комп'ютері становить 48 хв для $n=2^{64}$.

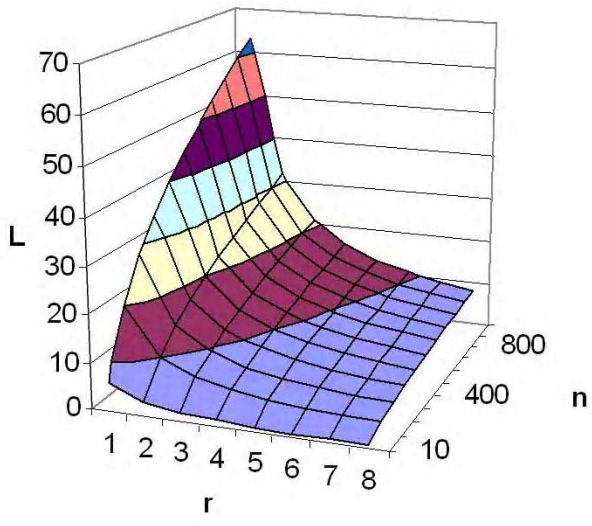

Рис. 6. Складність λ-методу Полларда

Таблиця 1. Час виконання програми, хв.

Кількість процесів, r	Метод	
	ρ-Полларда	λ-Полларда
4	6	10
5	3,5	6,5
6	2	4
7	1,5	2,5

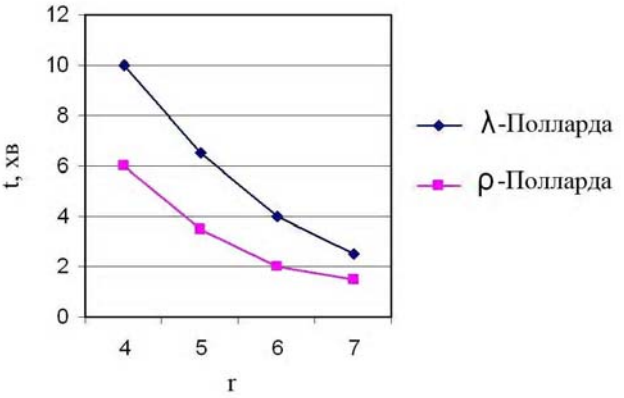

Рис. 7. Час виконання програми

Таблиця 2.Час виконання програми для різних n, хв.

r	$n=2^{64}$	$n=2^{73}$	$n=2^{84}$	$n=2^{96}$
4	22	41	–	–
5	14	26	–	–
6	11	19	38	–
7	10	15	25	37

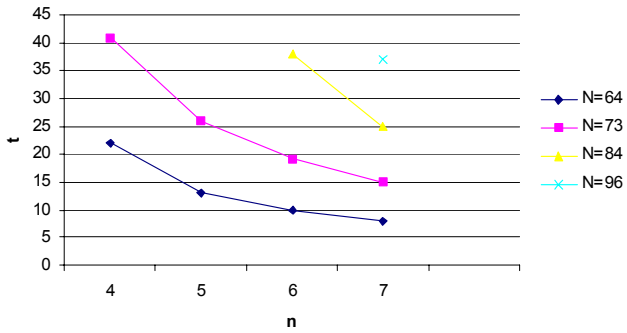

Рис. 8. Час виконання програми, хв.

З табл. 2 і графіка на рис. 8 видно, що програма криптоаналізу дозволяє істотно скоротити час обчислень.

Відомо, що можна прискорити обчислення за λ-методом Поларда, якщо відомий відрізок, на якому знаходиться значення дискретного логарифму [4]. У роботі [5] аналізується інший підхід – можливість використання λ-методу Полларда в тому випадку, коли не відомий відрізок, на якому лежить значення логарифму, шляхом розпаралелювання рішення алгоритму на довільну кількість обчислювальних вузлів r. При цьому весь діапазон, на якому проводиться пошук рішення, ділиться на r рівних частин. Кожен i-й обчислювальний вузол вирі-

шує завдання λ-методом Полларда так, як ніби розв'язання задачі дискретного логарифму лежить на i-му відрізку. Коли розв'язок знайдено одним з обчислювальних вузлів, інші свою роботу зупиняють. Результати обчислень представлені в табл. 3.

Таблиця 3. Залежність середнього прискорення паралельних обчислень від кількості обчислювальних вузлів r

Кількість обчислювальних вузлів r	1	2	3	4
Середнє прискорення обчислень	1	1,06	1,15	1,21

ВИСНОВКИ

Використання паралельних обчислень у криптоаналізі для прискорення методів ρ- і λ-Полларда знижує час виконання розрахунків. Але розглянуті методи розпаралелювання не дозволяють отримати значного прискорення обчислень, і не збільшують небезпеку злому при прийнятних величинах порядку базової точки. Надалі планується модернізація системи для дослідження інших методів розв'язання задачі дискретного логарифмування і порівняльного аналізу їх практичної складності обчислення.

СПИСОК ЛІТЕРАТУРИ

1. *Молдовян, Н. А.* Введение в криптосистемы с открытым ключом [Текст] / Н. А. Молдовян, А. А. Молдовян // С. Пб. : BHV, 2005. – 288 с.
2. *Василенко, О. Н.* Теоретико-числовые алгоритмы в криптографии [Текст] / О. Н. Василенко. – М. : МЦНМО, 2003. – 328 с.
3. *Андрущенко, Д. М.* Практическая оценка стойкости асимметричных криптосистем [Текст] / Д. М. Андрущенко, Г. Л. Козина, Д. М. Пиза // Проблемы информационной безопасности. – 2008. – № 1. – С. 57–62.
4. *Смарт, Н.* Криптография [Текст] / Н. Смарт . – М. : Техносфера, 2005. – 528 с.
5. *Андрущенко, Д. М.* О распараллеливании методов Полларда решения задачи дискретного логарифмирования [Текст] / Д. М. Андрущенко, Г. Л. Козина // VII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» : збірка тез доповідей учасників. Частина 1. – К., 2009. – С. 10–11.

Стаття надійшла до редакції 18.05.2011.

Андрущенко Д. М., Варава М. Ю., Неласая А. В.

РАСПАРАЛЛЕЛИВАНИЕ ρ- I λ-МЕТОДОВ ПОЛЛАРДА РЕШЕНИЯ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ.

Проведен анализ эффективности распараллеливания ρ- и λ- методов Полларда при решении задачи дискретного логарифмирования. Приводится теоретическая оценка времени выполнения задачи на параллельной системе. Проведено сравнение результатов практических и теоретических расчетов. Сделаны замеры времени выполнения распараллеленных методов.

Ключевые слова: методы Полларда, дискретный логарифм, распараллеливание, сложность криптоалгоритма, оценка сложности.

Andrushchenko D. M., Varava M. U., Nelasa G. V.

PARALLELIZATION OF ρ- AND λ- POLLARD'S METHODS FOR SOLVING THE DISCRETE LOGARITHM

The parallelization efficiency of ρ- and λ-methods of Pollard in solving the discrete logarithm is analyzed. The theoretical estimate of the time of the task on a parallel system is given. Comparison of the practical and theoretical calculations carried out. Timing performance threaded methods are made.

Key words: methods of Pollard's, discrete logarithm, paralleling, the complexity of the cryptographic algorithm, estimation of complexity.

УДК:681.5

Кулик А. С.[1], Лученко О. О.[2], Фирсов С. Н.[3]

[1]Д-р техн. наук, заведующий кафедрой Национального аэрокосмического университета им. М. Е. Жуковского «ХАИ»
[2]Генеральный директор-Главный конструктор Хартрон-Планта,
[3]Канд. техн. наук, доцент Национального аэрокосмического университета им. М. Е. Жуковского «ХАИ»

КОНЦЕПЦИЯ ОБЕСПЕЧЕНИЯ ЖИВУЧЕСТИ СПУТНИКОВЫХ СИСТЕМ УПРАВЛЕНИЯ ОРИЕНТАЦИЕЙ И СТАБИЛИЗАЦИЕЙ

Сформулированы основные положения обеспечения живучести спутниковых систем ориентации и стабилизации, базирующиеся на принципе самоорганизации посредством глубокого диагностирования аварийного функционального состояния и гибкого восстановления работоспособности объекта.

Ключевые слова: живучесть, диагностирование, нештатная ситуация, самоорганизация.

ВВЕДЕНИЕ

Расширение круга функциональных задач, решаемых современными космическими аппаратами, и увеличение сроков их активного существования возможно путем обеспечения эффективного и качественного функционирования их бортовых систем как в номинальных