УДК 629.7.05, 621.398

© Кукушкин С.С., Нестеровский И.С.
Kukushkin S., Nesterovskiy I.

# МЕТОДЫ НЕТРАДИЦИОННОГО ПРЕДСТАВЛЕНИЯ ДАННЫХ ОБРАЗАМИ-ОСТАТКАМИ И АНАЛИЗА ЭФФЕКТИВНОСТИ ИХ ПРИМЕНЕНИЯ

# NON-TRADITIONAL METHODS OF DATA IMAGES OF THE RESIDUAL AND ANALYZE THEIR PERFORMANCE

***Аннотация.*** *Статья посвящена проблеме повышения эффективности передачи ТМИ при использовании структурно-алгоритмических методов, использующих нетрадиционное представление передаваемых данных образами-остатками. Детально исследуются новые возможности по повышению качества и скрытности передаваемой телеметрической информации, появляющиеся при сравнении данных телеизмерений по двойному модулю: с использованием модулей-чисел и модулей-полиномов. Показаны основные преимущества подобных представлений и их недостатки, которые необходимо устранить. Сравнительный анализ различных альтернативных вариантов обеспечен на основе статистико-лингвистического анализа, использующего модернизированное частотно-ранговое представление словоформ.*

***Annotation.*** *The article is devoted to a problem of improving the efficiency of transmission of the TMI data using structural-algorithmic methods using non-traditional presentation of transmitted data residuals. Thoroughly investigate new opportunities to improve the quality and secrecy of transmit-ted telemetry information that appears when comparing data telemetry system for double module: using modules-numbers and modules-polynomials. The basic advantages of such representations and their shortcomings that must be addressed. Comparative analysis of various options provided on the basis of statistical and linguistic analysis, using today's rank-frequency representation of word forms.*

***Ключевые слова.*** *Телеметрия, нетрадиционное представление данных образами-остатками, восстановление и обработка цифровых сигналов, искаженных помехами.*

***Key words.*** *Telemetry, not the traditional presentation of data residuals, recovery and processing of digital signals distorted by noise.*

## Введение

В условиях жестких финансово-экономических ограничений на развитие и модернизацию измерительных комплексов космодромов значительная роль в повышении точностных характеристик измерений отводится алгоритмическим методам. При этом определяющее значение для повышения эффективности информационно-измерительного обеспечения (ИИО) испытаний и штатной эксплуатации РКТ приобретают новые методы представления, передачи и обработки данных измерений, составляющие основу новых измерительных, вычислительных и информационных технологий и ориентированные на широкое применение вычислительной технику (ВТ). В их числе методы разработанной нетрадиционной прикладной теории конечных полей [1], как системообразующей основы объединения различных принципов представления, передачи и обработки данных на принципиально новой научно-методической базе. Ее основу составляет конструктивная теорема об остатках (КТО) [1], а также обобщение различных результатов исследований в области теории чисел [2], эффективности систем счислений [3] и защищенности информации от несанкционированного доступа [4] и помех [5].

Классическая теория конечных полей [6] была приспособлена для решения только частных прикладных задач таких, например, как помехоустойчивое ко-

*Кукушкин Сергей Сергеевич – ведущий научный сотрудник 4 ЦНИИ Минобороны России, доктор технических наук, профессор, тел.+7(495)515-19-82.*
*Нестеровский Игорь Сергеевич – научный сотрудник 4 ЦНИИ Минобороны России, тел.+7(256)2-84-83.*

*Kukushkin Sergey – the main scientific employee 4 Central Scientific Research Institute Ministry of Defence of Russia, doctor of the technical sciences, professor. Ph.+7(495)515-19-82.*
*Nesterovskiy Igor – scientific employee 4 Central Scientific Research Institute Ministry of Defence of Russia.*

дирование передаваемой информации [5]. Поэтому, когда появилась необходимость в ее применении для решения проблем, сложившихся в существующем телеметрическом комплексе, то потребовалась ее принципиальная перестройка.

Вся разработанная теория, направленная на повышение качества ИТО испытаний вооружения и военной техники (ВВТ) и защиты данных от помех, могла бы оказаться бесполезной для практической реализации, если бы не были найдены в ходе проведенных исследований упрощенные алгоритмы преобразования и восстановления ТМИ, представленной образами-остатками [1]. Наиболее значительные исследования были проведены в направлении поиска таких замещающих математических конструкций (ЗМК), которые бы отличались от известных аналогов наибольшей простотой технической реализации. Примером подобных ЗМК является и адаптивный алгоритм восстановления в исходном виде данных, которые с целью повышения помехоустойчивости их передачи были представлены образами-остатками [1].

Потребность в ЗМК возникает всегда, когда попытка решения поставленной задачи классическими методами не приводит к успеху.

Так, в результате проведенных исследований было показано, что основные алгоритмы преобразования данных ТМИ в образы – остатки существенно упрощаются при использовании двоичного представления данных с использованием символов «0» и «1». Это свойство появляется только при представлении данных двоичным кодом. Ни одна из существующих теорий, кроме КТКП, не опускается до кодового уровня анализа и синтеза данных телеизмерений. Практически для всех теорий исходным базисом для создания новых алгоритмов является традиционная позиционная система счисления [3]. При этом во многих случаях считается, что она не подлежит ревизии.

Новые технологии представления и передачи данных базируются на представлении исходного сообщения (числа) $X$ образами-остатками $b_i$, получающимися в результате операции деления $X$ на модули сравнения $m_i$:

$$X \equiv b_i \,(mod\, m_i). \qquad (1)$$

Особенность нетрадиционного представления данных образами-остатками $b_i$ заключается в том, что последних может быть много $b_i$, $i = 1,2,...,k$. Их число определяется количеством использованных модулей сравнения $m_i$, $i = 1,2,...,k$. В этом случае говорят о представлении $X$ системой остаточных классов (СОК):

$$\begin{aligned} X &\equiv b_1 \,(mod\, m_1);\\ X &\equiv b_2 \,(mod\, m_2);\\ X &\equiv b_k \,(mod\, m_k). \end{aligned} \qquad (2)$$

Применительно к процессам, к числу которых относятся и телеметрируемые параметры (ТМП), формулы (1) и (2) записываются в следующем виде:

$$x(t) \equiv b_i(t)(mod\, m_i);\ i = 1,2,...,k. \qquad (3)$$

При этом для однозначного восстановления данных ТМИ произведение модулей сравнения необходимо выполнить условия $m_1 \times m_2 \times ... \times m_k \geq Ш$, где Ш – шкала представления значений ТМП.

## 1. Основные аналитические соотношения, относящиеся к представлению данных образами-остатками

В существующих телеметрических системах данные телеизмерений представлены информационными словами, имеющими разрядность от 8 до 10 бит. Шкала однозначного отображения всего набора данных, задаваемых двоичными $n$-разрядными кодами определяется от 0 до $2^n-1$. Следовательно, для байтовых слов она определяется значениями 0–255, при $n = 10$ Ш = 0–1023.

Если брать байтовую структуру слов, то в соответствии с конструктивной теорией конечных полей (КТКП), необходимо найти такие два числа, которые бы число 255 делилось без остатка с минимальной разницей между собой. Для приведенного примера это модули 15 и 17 ($15 \times 17 = 255$). Не сложно заметить, что в структуре данного разложения присутствует следующее известное алгебраическое тождество:

$$2^n - 1 = (2^{n/2} - 1)(2^{n/2} + 1). \qquad (4)$$

В свою очередь алгебраическое представление числа $(2^{n/2} - 1)$ можно разложить на следующие сомножители:

$$2^{n/2} - 1 = (2^{n/4} - 1)(2^{n/4} + 1). \qquad (4^*)$$

При больших значениях $n$, определяющих разрядность кодовых комбинаций $C_i$ этот процесс может быть продолжен до получения минимального модуля сравнения, равного 3 ($m_1 = 3$).

Далее из следующих друг за другом словизмерений $W_1, W_2, ..., W_s$ могут быть составлены информационные предложения, фразы или пакеты данных. При этом зачастую нужную информацию несет не само отдельное информационное слово $W_i$, а их совокупность (предложения, фразы или пакеты данных).

*Пример* 1. В качестве примера приведем структуру одной из фраз, используемой при передаче информации СРНС ГЛОНАСС:

**45 4C** 30 30 39 27 1F 2E | 10 40 09 28 14 20 **0D 0A**;
**0100.0101|0100.1100**|0011.0000|0011.0000|0011.1001|
0010.0111|**0001.1111|0010.1110**| ;
0001.0000|0100.0000|0000.1001|0010.1000|0001.0100|
0010.0000|**0000.1101|0000.1010| .**

Всего сообщений в фразе – 16 байт, из них 2 байта – заголовок (стоит в начале), 2 байта – маркировка окончания (размещены в конце) и информационных – 12 байт.

### 2. Преобразование данных и информационных предложений с использованием образов-остатков

Для демонстрации новых технологий с использованием нетрадиционного представления данных образами-остатками примем, что число байтовых слов, объединенных в предложение, равно 4 (s = 4):

$W_1 = <1011\ 1111>_2 = <191>_{10}$;

$W_2 = <1011\ 1111>_2 = <134>_{10}>_2$;

$W_3 = <1010\ 0000>_2 = <160>_{10}$;

$W_4 = <1101\ 1111>_2 = <223>_{10}>_2$.

Предположим, что они объединены в информационное предложение

$$И = < W_1, W_2, W_3, W_4 >_2. \quad (5)$$

При первом преобразовании, связанном с нахождение образов-остатков по модулям числам $m_1$ = 15 и $m_2$= 17, получим

$$И_{пр1}^{(СОК)} = < \boldsymbol{b_{11}}, b_{12}; \mathbf{b_{21}}, b_{22}; \boldsymbol{b_{31}}, b_{32}; \boldsymbol{b_{41}}, b_{42} >_2. \quad (6)$$

Далее объединяем полученные образы-остатки в систему с использованием формальных многочленов

$$f_1(x) = b_{11}\cdot x^3 + b_{21}\cdot x^2 + b_{31}\cdot x + b_{41}\cdot (mod 15); \quad (7)$$

$$f_2(x) = b_{12}\cdot x^3 + b_{22}\cdot x^2 + b_{32}\cdot x + b_{43}\cdot (mod 17). \quad (8)$$

Затем выбираем модули-полиномы, например, $m_1(x) = x^2 + x$; $m_2(x) = x^2 + x + 1$ и поочередно делим на них многочлены (7) и (8) (табл. 1). Результат первичного кодирования с использованием модулярной арифметики (сравнения по модулям-числам $m_1$ =15 и $m_2$ =17) представлен в табл.1 значениями $X_{ci}$ = {180, 239, 167, 210} вместо исходной значений последовательности значений $X_i$={191, 134, 160, 223}.

Его суть заключена в том, что последовательность измеренных значений (для примера следующие друг за другом четыре значения ТМП $x(t)$: 107, 109, 113, 116 преобразованы в образы-остатки $b_1$ (*mod 15*) и $b_2$ (*mod 17*), каждый из которых представлен четырьмя двоичными разрядами.

Далее из них составлены новые байтовые слова-измерения: $X_п = <b_i, b_{i+2}>_2$, образующие новую последовательность данных при традиционном их восстановлении, как обычного байтового слова-измерения: 37, 71, 139, 190.

При этом имеется возможность определения ло-

Таблица 1

**Результаты сравнения данных по двойному модулю**

| Форма представления $X(t)$ | Информационные слова - $<X_i>_2$, $<X_i>_{10}$, $<X_{Ci}>_2 = <a_1$ *-старшее полуслово,* $a_2$ *- младшее полуслово* $>_2$ ,$<X_{Ci}>_2 = = <b_1$ *-первое полуслово-остаток,* $b_2$ *- второе полуслово-остаток* $>_2$ | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Двоичная (байтовая) $<X_i>_2$ | 1011 1111 | | 1000 0110 | | 1010 0000 | | 1101 1111 | |
| Десятичная $<X_i>_{10}$ | $X_i$=191 | | $X_{i+1}$=134 | | $X_{i+2}$=160 | | $X_{i+3}$=223 | |
| Полусловами | $a_1$ | $\boldsymbol{a_2}$ | $a_1$ | $\boldsymbol{a_2}$ | $a_1$ | $\boldsymbol{a_2}$ | $a_1$ | $\boldsymbol{a_2}$ |
| Двоичная $<X_i>_2$ | 1011 | **1111** | 1000 | **0110** | 1010 | **0000** | 1101 | **1111** |
| Образы-остатки $X_C(t)$ | $m_1$=15 $b_{1i}$=11 | $m_2$=17 $b_{2_i}$ = 4 | $m_1$=15 $b_{1_{i+1}}$ = 14 | $m_2$=17 $b_{2_{i+1}}$ = 15 | $m_1$=15 $b_{1_{i+2}}$ = 10 | $m_2$=17 $b_{2_{i+2}}$ =7 | $m_1$=15 $b_{1_{i+3}}$ =13 | $m_2$=17 $b_{2_{i+3}}$ =2 |
| Полусловами | $b_{1_i}$ | $b_{2_i}$ | $b_{1_{i+1}}$ | $b_{2_{i+1}}$ | $b_{1_{i+2}}$ | $b_{2_{i+2}}$ | $b_{1_{i+3}}$ | $b_{2_{i+3}}$ |
| Двоичная $<X_C>_2 = =< b_1, b_2 >_2$ | 1011 | 0100 | 1110 | 1111 | 1010 | 0111 | 1101 | 0010 |
| Десятичная $<X_C>_{10} = =< b_1, b_2 >_{10}$ | $X_{C_i}$ = 180 | | $X_{C_{i+1}}$ = 239 | | $X_{C_{i+2}}$ = 167 | | $X_{C_{i+3}}$ = 210 | |

кальных свойств непрерывности (корреляционной взаимосвязи) переданных значений. Она устанавливается на основе определения разностей между предшествующими и последующими значениями в традиционной и новой форме.

Для первой последовательности абсолютные разности равны

$\Delta_i = |107-109| = 2$; $\Delta_{i+1} = |109-113| = 4$;

$\Delta_{i+2} = |113-116| = 3$.

Для второй (преобразованной) последовательности

$\Delta_{n(i)} = |37-71| = 34$; $\Delta_{n(i+1)} = |71-139| = 68$;

$\Delta_{n(i+2)} = |139-190| = 51$.

Определяя отношение $k$, получим

$$k = \frac{\Delta_{n(i+m)}}{\Delta_{i+m}} = 17. \quad (9)$$

Таким образом, число $k$, близкое к 17, можно выбрать в качестве критерия непрерывности дискретных значений ТМП. Кроме того, отмеченная особенность может составить основу нового подхода к декодированию данных, позволяющему обнаруживать и исправлять ошибки передачи ТМИ.

На основе данного критерия также осуществляется контроль достоверности приема полуслов-остатков в условиях «безызбыточного» помехоустойчивого кодирования. Здесь понятие «безызбыточного» помехоустойчивого кодирования используется в том смысле, что разрядность исходных и преобразованных слов-измерений остается неизменной. Однако фактическая избыточность информации при этом присутствует. Она связана с переходом от простой системы позиционного принципа представления слов-измерений к новой смешанной системе счисления, позиционность в которой сохраняется только внутри малых информационных элементов, к числу которых относятся образы-остатки. При этом сами образы-остатки могут меняться местами и это никак не сказывается на результатах обратного преобразования (восстановления) ТМИ. В этом заключается основной принцип непозиционной системы счисления.

### 3. Системы счисления и основные подходы по их выбору в адаптивных системах передачи информации

Известный пример простейшей смешанной системы – это римская система счисления. В ней, например, числу «30» в привычной арабской системе написания соответствует непозиционный его аналог «XXX». Если, например, при передаче поменять местами цифры 0 и 3, то получим значение «03». Такие превращения (ошибки) могут быть при передаче и при приеме информации на фоне помех. Поскольку они не контролируемы, то ошибка при приеме смысловой информации может быть недопустимо большой (по отношению к приведенному примеру в $10^{n-1}$ раз, где $n$ – разрядность передаваемых десятеричных слов). Для приведенного примера $n$=2 и ошибка равна $\delta$=10. В случае двоичных слов ошибка определяется величинами $2^{n-1}$, где $n$ – порядковый номер значения символа «0» или «1», начиная с младшего разряда. В случае непозиционного представления этого же числа «XXX» символы можно менять местами, а получаемый при этом результат останется неизменным. Однако римская система счисления избыточна и это также следует из приведенного примера.

Однако прикладные задачи использования систем счисления при передаче информации требуют, как минимум, следующего:

- должны быть сохранены по максимуму преимущества как одной, так и другой системы;
- информационная нагрузка символа в новой смешанной системе счисления должна быть максимальной (это значит, что количество информации, переносимой одним символом, должно быть наибольшим при заданных ограничениях на разрядность слов-измерений $n=n_{тр}$, время передачи ТМИ $T \le T_{тр}$, полосу пропускания радиоканала $\Delta f \le \Delta f_{зад}$, и скорость передачи данных $R \le R_{зад}$.

Последнее требование в формализованном виде может быть записано следующим образом:

$$I_{(0,1)} \to U(A_{сист.счил}) \to max; \quad (10)$$
$$n = n_{тр}; T \le T_{тр}; \Delta f \le \Delta f_{зад}; R \le R_{зад},$$

где $I_{(0,1)}$ – эквивалентная информационная нагрузка двоичных символов, которая характеризует, насколько повышается информационная значимость двоичных символов по сравнению с представлением данных простым двоичным кодом;

$U$ – оператор выбора подходящей системы счисления (представления и модуляции данных, подлежащих передаче);

$A_{сист.счил}$ – алгоритм формирования системы счисления.

### 4. Основные подходы к оцениванию эффективности систем счисления и проблемно-ориентированному выбору наиболее предпочтительных альтернатив

Известный подход к оцениванию эффективности систем счисления приведен в работе [3]. При этом под экономичностью понимается тот запас чисел, для записи которого в данной системе представления требуется определенное количество символов. Воспользуемся ме-

тодикой, приведенной в работе [3], для оценивания эффективности системы счисления, основу которой составляет представление последовательности чисел результатами сравнений: $b_1(mod\ 38)$ и $b_2(mod\ 39)$. Например, для того, чтобы в десятичной позиционной системе счисления записать 1000 чисел (от 0 до 999), необходимо 30 символов (по 10 символов для каждого разряда) (табл. 2) [3]. Выбор модулей сравнения 38 и 39 был сделан из следующих противоречивых соображений:

• числовой диапазон значений должен быть не менее 1000 (Ш = 0–999) для обеспечения большей сравнимости с примером, приведенным в работе [3], с одной стороны, и в то же время количество символов $n$, которые используются для его однозначного представление должно быть минимальным. В итоге мы приходим к следующей минимаксной задаче оптимизации:

$$Ш \to \max, \text{ а } n \to \times \min. \qquad (11)$$

Ее решение представлено в табличном виде (табл. 2 и 3).

Таблица 2

**Традиционное позиционное представление числа**

| | | |
|---|---|---|
| 9 | 9 | 9 |
| 8 | 8 | 8 |
| 7 | 7 | 7 |
| 6 | 6 | 6 |
| 5 | 5 | 5 |
| 4 | 4 | 4 |
| 3 | 3 | 3 |
| 2 | 2 | 2 |
| 1 | 1 | 1 |
| 0 | 0 | 0 |

30 символов

Таблица 3

**Нетрадиционное (смешанное) представление числа**

| $b_1$ | $m_1$ | $b_2$ | $m_2$ |
|---|---|---|---|
| | 9 | | 9 |
| | 8 | | 8 |
| | 7 | | 7 |
| | 6 | | 6 |
| | 5 | | 5 |
| | 4 | | 4 |
| 3 | 3 | 3 | 3 |
| 2 | 2 | 2 | 2 |
| 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 0 |

28 символов

Табл. 2 соответствует традиционной позиционной системе счисления, которая используется и при передаче информации. Из нее следует, что для того, чтобы отобразить любое число в шкале $Ш_{тр}$ = 0–999 необходимо три разряда по 10 символов от 0 до 9 в каждом из них. Итого 30 символов. В табл. 3 представлен пример использования предлагаемой смешанной десятичной системы счисления, удовлетворяющей условиям минимаксной оптимизации (11). При этом шкала однозначного представления чисел расширена до значения $Ш_{СОК}=m_1 \times m_2 = 38\times39 = 1482 > 1000$, число символов $n$, необходимых для отображения натурального ряда чисел в пределах $Ш_{СОК}$ уменьшилось с 30 до 28.

Если предположить $n$ равным, то даже в этом случае предлагаемая нетрадиционная система счисления на основе представления данных в СОК в $k_{сч}=\frac{1482}{1000}=1{,}482$ раза эффективнее существующей позиционной. Применительно к ТМИ этот результат можно интерпретировать следующим образом. При представлении данных телеизмерений $X$ двумя образами-остатками $b_1$ и $b_3$ по четыре разряда в каждом (двумя полусловами) при модулях сравнения $m_1 = 15$ и $m_3 = 17$, вместо традиционно используемого позиционного представления слов байтами (8 разрядами), плотность упаковки передаваемой информации в групповом телеметрическом сигнале (ГТС) той же структуры повышается в $k_{сч} = 1{,}482$ раз.

Этот же результат можно интерпретировать в рамках существующей теории расчета эффективности различных систем передачи информации и как эквивалентное увеличение информационной нагруженности (насыщен-ности) каждого из передаваемых символов двоичного кода в $k_{сч} = 1{,}482$ раз.

Таким образом, неявно присутствующая избыточность в передаваемых данных обусловлена тем, что используется нетрадиционная смешанная система счисления при представлении данных телеизмерений. Поэтому противоречий с теорией классического помехоустойчивого кодирования также нет.

## 5. Предложения по кодированию данных в системе остаточных классов (СОК)

В общем случае основу кодирования составляет система остаточных классов (СОК), которая связана с представлением данных $X$ образами-остатками, например, $b_1$, $b_2$, $b_3$, полученными при выполнении операций деления $X$ на модули сравнения $m_1$, $m_2$, $m_3$.

$$\begin{aligned} &X \equiv b_1(mod\ m_1),\ m_1 = 2^n-1;\\ &X \equiv b_2(mod\ m_2),\ m_2 = 2^n;\\ &X \equiv b_3(mod\ m_3),\ m_3 = 2^n+1. \end{aligned} \qquad (12)$$

Синтезированные на их основе коды идеально

подходят для исправления, как одиночных ошибок, так и групповых ошибок. Известные коды такой способностью не обладают.

Оптимальными для случая кодирования байтовых слов ($2n = 8$ бит) будут следующие модули:

$m_1 = 2^4 - 1 = 15$; $m_2 = 2^4 = 16$; $m_3 = 2^4 + 1 = 17$.

Оптимальность такого выбора определяется следующими факторами:

• описанными выше свойствами произведения модулей $m_1 \times m_3 = (2^n - 1)(2^n + 1) = 2^{2n} - 1$, в результате которого обеспечивается возможность восстановления данных в шкале $(0 - 2^{2n})$(для байтовых слов в шкале 0–255);

• возможностью замены операции деления $X$ на модули сравнения $m_1$, $m_3$ на ЗМК, основу которой составляет сложение старших и младших полуслов (полубайт) $a_1$ и $a_2$ в прямом и инверсном виде (при этом остаток $b_2$ по модулю $m_2 = 2^n$ представляет собой младшее полуслово $a_2$ ($a_2 = b_2$).

На рис. 1 приведены графические отображения одного и того же ТМП:

а) представленного в традиционном виде $x(t)$ (вверху);

б) составленного из двух образов-остатков $x_п(t) = <b_1(t), b_3(t)>_2$, где $<>_2$ – знак объединения образов-остатков $b_1(t)$, $b_3(t)$ в новое слово-измерение той же разрядности, что и исходное $x(t)$.

$K_ш^{(тр)} = (32 - (-5))/512 = 37/512 = 0{,}072$.

После преобразований

$K_ш^{(СОК)} = (255 - (-100))/512 = 355/512 = 0{,}693$.

Коэффициент $k = K_ш^{(СОК)} / K_ш^{(тр)}$ полезного использования отведенной шкалы телеизмерений $Ш$ преобразованного ТМП $x_n(t) = <b_1(t), b_3(t)>_2$ может быть выбран в качестве одного из критериев эффективности телеметрической системы. Для приведенных на рис. 1 примеров различного представления одного из реальных ТМП он равен: $k = 0{,}693/0{,}072 = 9{,}625$. Эффект значительный. Ничего подобного нельзя достичь при использовании традиционного подхода.

Кроме того, одно из преимуществ нетрадиционного представления данных образами-остатками заключается в том, что количество различных проблемно-ориентировочных преобразований может быть большим. Это свойство составляет основу построения новой системы структурно-алгоритмической защиты ТМИ от несанкционированного доступа (НСД).

## 6. Использование дополнительного преобразования информационных предложений, фраз и пакетов данных на основе сравнения по модулям-полиномам

Составим информационное предложение ($И_{пр}$) из следующих четырех байтовых слов:

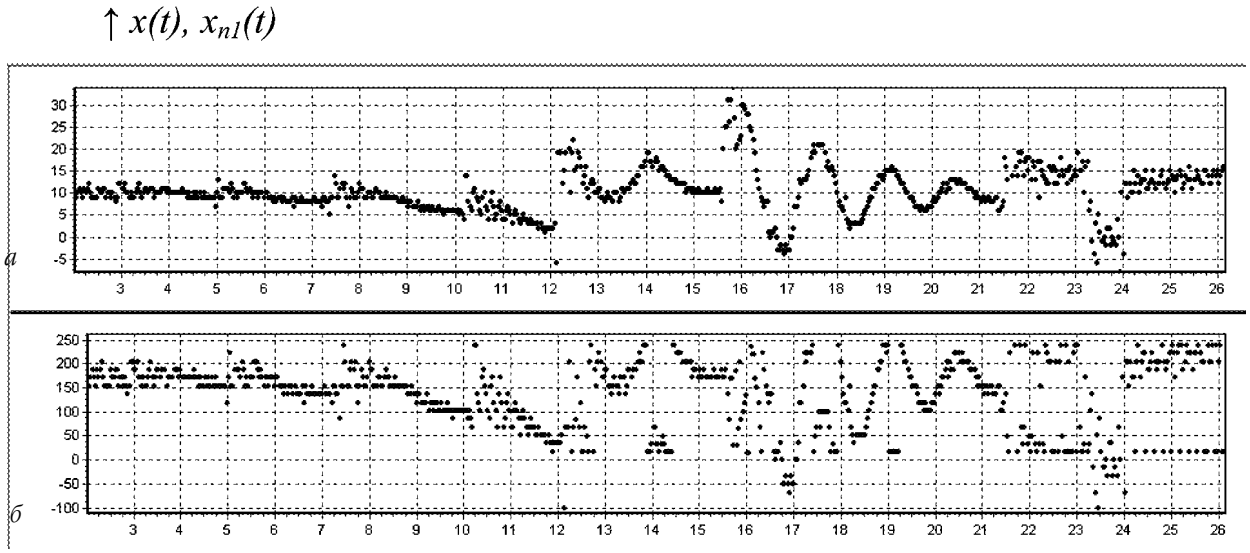


Рис. 1. Графические отображения одного и того же ТМП:
а – представленного в традиционном виде $x(t)$; б – составленного из двух образов-остатков $x_n(t) = <b_1(t), b_3(t)>2$

Исходные значения ТМП были представлены в узком амплитудном диапазоне (от – 5 до 32), в то время как исходная шкала $Ш$ представления данных телеизмерений представлена в интервале от – 255 до +255. Коэффициент полезного использования шкалы телеизмерений $Ш$ равен

$$И_{пр} = \{W_1; W_2; W_3; W_4\} = \{142_{10}, 58_{10}, 36_{10}, 200_{10}\} => \quad (13)$$
$$=> \{<10001110>_2, <00111010>_2, <00100010>_2, <11001000>_2\},$$

где $W_1; W_2; W_3; W_4$ – слова, представленные в традиционном виде, и их численные, и кодовые значения.

Представим эти слова в виде СОК: 7 + 6; 13 + 7; 6 + 2; 5 + 13. Выделим все остатки по модулю 15 и соста-

вим формальный многочлен третьей степени

$f_1(x) = 7x^3 + 13x^2 + 6x + 5(mod\ 15)$;

$f_2(x) = 6x^3 + 7x^2 + 2x + 13\ (mod\ 17)$.

Поделим каждое уравнение на следующие выбранные модули-полиномы:

$m_1(x) = x^2 + x$ и на $m_2(x) = x^2 + x + 1$.

В результате деления получают следующие полиномы-остатки:

$$\boldsymbol{b_1^{(1)}(x)=\alpha_{11}x+\alpha_{12}};\ b_1^{(2)}(x)=\alpha_{21}x+\alpha_{22};$$
$$b_2^{(1)}(x)=\beta_{11}x+\beta_{12};\quad \boldsymbol{b_2^{(2)}(x)=\beta_{21}x+\beta_{22}}. \qquad (14)$$

Передаче подлежат преобразованные слова, составленные из коэффициентов

$$И_{пр2}^{(f)} = <\alpha_{11},\alpha_{12},\alpha_{21},\alpha_{22},\beta_{11},\beta_{12},\beta_{21},\beta_{22}>_2 \qquad (15)$$

Применительно к данному примеру результаты кодирования будут иметь следующий вид:

$\alpha_{11}=\mathbf{0}$; $\alpha_{12}=\mathbf{5}$; $\alpha_{21}=8$; $\alpha_{22}=14$;

$\beta_{11}=\mathbf{1}$; $\beta_{12}=\mathbf{13}$; $\beta_{21}=12$; $\beta_{22}=12$.

При переходе к двоичному коду получим следующее преобразованное информационное предложение (14):

$$И_{пр2}^{(f)}=\{W_{1пр};\ W_{2пр};\ W_{3пр};\ W_{4пр}\} =$$
$$=\{0 + 5;\ 8 + 14;\ 1 + 13;\ 12 + 12\} = \qquad (14^*)$$
$$=\{<0000.0101>_2, <1000.1110>_2, <0001.1101>_2, <1100.1100>_2\},$$

где $W_{1пр}$; $W_{2пр}$; $W_{3пр}$; $W_{4пр}$ – новые (преобразованные) слова той же разрядности и значения составляющих их образов-остатков.

Декодирование может быть выполнено двумя способами:

1 на основе конструктивной теоремы об остатках [15];

2 с использованием следующих аналитических соотношений, позволяющих, например, перейти от переданных коэффициентов полиномов-остатков $\alpha_{11},\alpha_{12},\alpha_{21},\alpha_{22}$ к результатам сравнения $b_{1i}$, $b_{1(i+1)}$, $b_{1(i+2)}$, $b_{1(i+3)}$, полученных по модулю $m_1 = 15$ для каждого из преобразованных слов:

$$b_{1i} = \alpha_{21} - \alpha_{11};$$
$$b_{1(i+1)} = \alpha_{21} + \alpha_{22} - \alpha_{12} - \alpha_{11};$$
$$b_{1(i+2)} = \alpha_{21} + \alpha_{22} - \alpha_{12}; \qquad (16)$$
$$b_{1(i+3)} = \alpha_{22}.$$

Из (3) следует следующее проверочное уравнение:

$$b_{1(i+2)} - b_{1(i+1)} = \alpha_{11};$$
$$b_{1i} - b_{1(i+1)} = \alpha_{12} - \alpha_{22}; \qquad (17)$$
$$b_{1i} = \alpha_{21} - \alpha_{11}.$$

В то же время $m_1(x) = x^2 + x = x(x+1)$. Это значит, что

$$\boldsymbol{\gamma_{11}(x) \equiv 5\ (mod\ x)} \text{ и } \boldsymbol{\gamma_{12}(x) \equiv 5\ (mod\ (x+1))}; \qquad (18)$$
$$\boldsymbol{\gamma_{21}(x) \equiv 13\ (mod\ x)} \text{ и } \gamma_{21}(x) \equiv \boldsymbol{12\ (mod\ (x+1))}. \qquad (19)$$

Это означает, что сформированная кодовая последовательность дополняется остатками от сравнения по модулям $m_{11}(x) = x$ и $m_{12}(x) = x + 1$.

При этом новая избыточная кодовая конструкция формируется в результате объединения данных (14) и (15):

$$И_{пр2}^{(физб)}=<\alpha_{11},\alpha_{12},\alpha_{21},\alpha_{22},\beta_{11},\beta_{12},\beta_{21},\beta_{22}>_2 \qquad (15^{**})$$

При этом проверочные уравнения при безызбыточном кодировании

$$b_{1(i+2)} - b_{1(i+1)} = \alpha_{11};$$
$$b_{1i} - b_{1(i+1)} = \alpha_{12} - \alpha_{22};$$
$$b_{1i} = \alpha_{21} - \alpha_{11}. \qquad (17^*)$$
$$b_{2(i+2)} - b_{2(i+1)} = \beta_{11};$$
$$b_{2i} - b_{2(i+1)} = \beta_{12} - \beta_{22};$$
$$b_{2i} = \beta_{21} - \beta_{11}. \qquad (20)$$

будут дополнены следующими соотношениями:

$$b_{1(i+3)} = \alpha_{22} = \gamma_{11};\ b_{2(i+3)} = \beta_{22} = \gamma_{13};$$
$$-b_{1i} + b_{1(i+1)} - b_{1(i+2)} - b_{1(i+3)} = \gamma_{12}; \qquad (21)$$
$$-b_{2i} + b_{2(i+1)} - b_{2(i+2)} - b_{2(i+3)} = \gamma_{22}.$$

В результате получаем помехоустойчивый код с 50% избыточностью данных, который обладает способностью не только обнаружения, но и исправления ошибок.

Один из вариантов графического представления предлагаемого помехоустойчивого кодирования ТМП представлен на рис. 2.

В результате помехоустойчивого кодирования разрушены корреляционные связи между значениями ТМП, что необходимо было сделать в рамках такой процедуры, как рандомизация данных формированного ГТС. Она необходима для повышения устойчивости синхронизации данных ТМИ при их приеме.

В рассматриваемом случае она совмещена с операцией помехоустойчивого кодирования ТМИ.

## Заключение

В результате проведенных исследований показано, что один из наиболее перспективных методов оптимизационного разрешения существующих противоречий ИТО испытаний РКТ связан с нетрадиционных представлением данных образами-остатками. Наиболее подробно рассмотрена новая технология, связанная с формализованным описанием совокупности кодовых конструкций, представляющих информационные предло-жения, фразы и пакеты данных, формальными многочленами и с переходом к передаче в линию связи коэффициентов полиномов-остатков, которые представляют собой результат деления формальных многочленов на полиномы-модули. При этом по сравнению с классической теорией конечных полей не накладываются жесткие ограничения, требующие, чтобы модули-полиномы представляли собой неприводимые многоч-

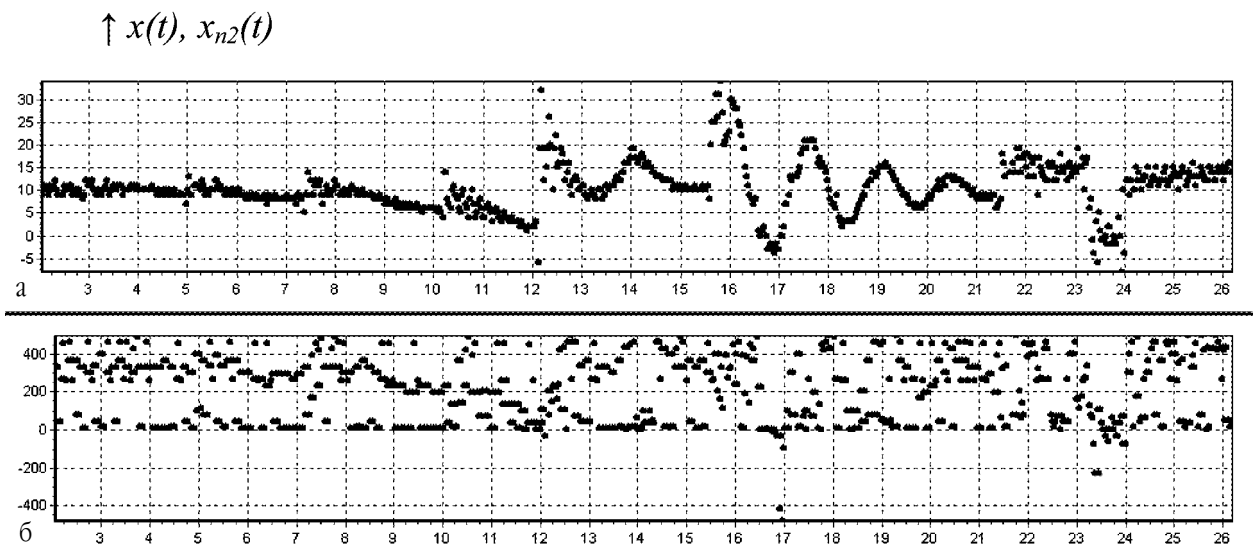


Рис. 2. Графические отображения одного и того же ТМП:
а – представленного в традиционном виде x(t); б – составленного из коэффициентов полиномов-остатков

лены. Благодаря этому существенно упрощена практическая реализация предлагаемых технологий.

*Литература*

*1. Кукушкин С.С. Теория конечных полей и информатика: т.1 «Методы и алгоритмы, классические и нетрадиционные, основанные на использовании конструктивной теоремы об остатках», - М.: МО РФ, 2003 – 284с.*
*2. Виноградов И.М. Основы теории чисел. - М.: Наука, 1980. - 118с.*
*3. Фомин С.В. Системы счисления. М.: Наука. Главная редакция физи-ко-математической литературы, 1980. - 48с.*
*4. Диффи У., Хелман М. Защищенность и имитостойкость: / Введение в криптографию // ТИИЭР, том 67, №3, 1979.*
*5. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Мир, 1976. – 593с.*
*6. Лидл Р., Нидеррайтер Г. Конечные поля. В 2-х томах. Пер с англ. - М.: Мир, 1988. - 882с.*

Материал поступил в редакцию 24. 03. 2011 г.