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

Velts Oksana Vladimirovna – e-mail: velts-yatsenco@yandex.ru; 33, Chehova street, fl. 66, Stavropol, 355000, Russia; phone: +78652944241; the department of information science; senior lecturer.

УДК 631.8

И.А. Калмыков, А.Б. Саркисов, А.В. Макарова

ТЕХНОЛОГИЯ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ С ИСПОЛЬЗОВАНИЕМ МОДУЛЯРНОГО ПОЛИНОМИАЛЬНОГО КОДА

Целью исследований является разработка новой технологии цифровой обработки сигналов (ЦОС), применение которой позволяет, за счет использования целочисленной непозиционной математической модели ЦОС, обеспечить высокоскоростную обработку сигналов в условиях воздействия помех и отказа оборудования. Возрастание требований к временным характеристикам современных систем ЦОС привело к созданию вычислительных устройств (ВУ), использующих параллельные вычисления. Однако при этом возникает следующая проблема: с одной стороны, постоянный рост требований к скоростным характеристикам ВУ приводит к необходимости организации параллельных вычислений, а с другой стороны, при этом увеличивается частота возникновения отказов и возрастает время простоя, вызванное трудностью отыскания неисправности.

Для решения данной проблемы в работе предлагается использовать математическую модель ЦОС, использующую модулярный полиномиальный код (МПК), который за счет распараллеливания на уровне операций и обработки малоразрядных данных позволяет не только увеличить скорость вычислений, но и обеспечивает получение корректного результата в условиях воздействия помех при передаче и отказа оборудования.

Цифровая обработка сигналов; ортогональные преобразования сигналов в кольце полиномов; модулярный полиномиальный код; коррекция ошибки; позиционные характеристики.

I.A. Kalmykov, A.B. Sarkisov, A.V. Makarova

TECHNOLOGY OF THE DIGITAL PROCESSING SIGNAL WITH USE MODULAR POLYNOMIAL CODE

The aim of research is a development to new technology of the digital processing signal (COS), which using allows, through the use of integer no positional mathematical model COS, provide speediest processing a signal in condition of the influence of the hindrances and refusal of the equipment. Increasing of requirements to the temporal characteristics of modern systems of COS led to the creation of computing devices (VU), using parallel computing. However, this raises the following problem: on the one hand, steady growth of requirements for high-speed characteristics of VU leads to the necessity of organization of parallel computations and on the other hand, this increases the frequency of occurrence of failures and increases downtime caused by the difficulty of finding fault.

To solve this problem it is suggested to use a mathematical model of a COS that uses modular polynomial code (MPC), which is due to parallelization at the level of operations and processing of small category data allows not only to increase speed of calculations, and ensures obtaining the correct result in the conditions of influence of interference during transmission and equipment failure.

Digital signal processing; the orthogonal transformation of signals in the ring of polynomials; modular polynomial code; correction of errors; positive institutional characteristics.

Введение. На современном этапе развития цивилизации информация играет ключевую роль в функционировании общественных и государственных институтов. Информационная среда, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности государства.

Широкое внедрение современных информационных технологий во все области хозяйственной и духовной жизни приводит к возрастанию значения защиты информационных ресурсов, которые являются объектом сбора, обработки передачи и хранения. Особо наглядно это проявляется в системах передачи и обработки сигналов.

Современный этап применения вычислительных устройств в этих системах показал, что использование методов ЦОС позволяет относительно легко обеспечить высокую помехоустойчивость систем обработки данных, необходимую точность и разрешающую способность, простое сопряжение подсистем обработки, стабильность параметров тракта обработки информации и ряд других преимуществ [1-5]. При этом задачи цифровой обработки сигналов требуют выполнение в реальном масштабе времени больших объемов вычислений над большими массивами данных. Добиться качественных изменений в возможностях современных систем передачи и обработки данных можно за счет применения новой математической модели реализации ортогональных преобразований сигналов в алгебраических модульных системах. При этом такая технология ЦОС должна не только повысить скорость и точность обработки сигналов, но и обеспечить отказоустойчивость вычислительного устройства цифровой обработки сигналов.

Постановка задачи исследования. Важность задач ЦОС делает целесообразной разработку специализированных устройств для их решения. При этом эффективность работы системы цифровой обработки сигналов во многом определяется математической моделью ЦОС.

В настоящее время все технические реализации ВУ ЦОС используют несколько математических моделей, которые можно разделить на следующие группы. Основу первой составляют математические модели, базирующиеся на реализации ортогональных преобразований сигналов над полем комплексных чисел, в частности дискретном преобразовании Фурье (ДПФ) и его быстрых алгоритмов. Так в системах широкополосного беспроводного доступа (ШБД) для борьбы с помехами при многолучевом приеме применяется технология ортогонального частотного мультиплексирования OFDM. Технически метод OFDM реализуется путем выполнения обратного дискретного преобразования Фурье (Fast Fourier Transform, FFT) в модуляторе передатчика и прямого дискретного преобразования Фурье – в демодуляторе приемника приемопередающего устройства [1–3].

Однако реализация быстрого преобразования Фурье характеризуется наличием двух вычислительных трактов и предопределяет значительные погрешности при вычислении значений спектральных коэффициентов в поле комплексных чисел, обусловленных тем, что поворачивающие коэффициенты представляют собой иррациональные числа.

Во вторую группу входят математические модели ЦОС, обладающие свойством конечного кольца и поля. Если значение входного сигнала $x(nT)$ рассматривать как подмножество других алгебраических систем, обладающих структурой кольца или конечного поля Галуа, то реализацию ортогональных преобразований сигналов можно свести к теоретико-числовым преобразованиям (ТЧП), определяемым в пространстве кольца вычетов целых чисел по модулю *M*. Однако основным недостатком ТЧП является жесткая связь между точностью вычислений, размерностью входного вектора *x(nT)* и значением модуля М. Даже небольшой динамический диапазон входных сигналов требует больших значений модуля *M*, а значит арифметическое устройство, реализующее ортогональные преобразования сигналов, должно иметь большую разрядную сетку.

В подавляющем большинстве приложений задача цифровой обработки сигналов сводится к нахождению значений ортогонального преобразования конечной реализации сигнала для большого числа точек, что предопределяет повышенные

требования к разрядности вычислительного устройства. Решить данную проблему можно за счет перехода от одномерных вычислений к многомерным. В основу данного преобразования положена китайская теорема об остатках (КТО) [6–10].

Для эффективной реализации ортогональных преобразований высокой точности необходимо доказать возможность реализации ДПФ в кольце полиномов. Пусть имеем кольцо полиномов *P(z)*, с коэффициентами в виде элементов поля *GF(p),* определяющего точность вычисления ортогональных преобразований сигналов. Положим, что кольцо разлагается в сумму

$$P(z) = P_1(z) + P_2(z) + ... + P_n(z), \quad (1)$$

где $P_l(z)$ – локальное кольцо полиномов, образованное неприводимым полиномом $p_l(z)$ над полем *GF(p); l=1, ..., n.*

Тогда в данной системе существует ортогональное преобразование, представляющее собой обобщенное ДПФ, если выполняются условия:

1. $\beta_i(z)$ – первообразный элемент порядка *d* для локального кольца $P_l(z)$, где *l=1, ...,m.*

2. *d* имеет мультипликативный обратный элемент d^*.

Ортогональное преобразование является обобщенным ДПФ для кольца вычетов *P(z)* если существуют преобразования над конечным кольцом $P_l(z)$

$$X_l^k(z) = \sum_{n=0}^{d-1} x_l^n(z)\beta_l^{kn}(z), \quad (2)$$

где $\left\{ \; X_l^k(z), x_l^n(z), \beta_l^{kn}(z) \; \right\} \in P_l(z)$, *l=1,2,...,m; k=0,1,...d-1.*

Полученная циклическая группа имеет порядок *d*. Поэтому ДПФ над $P_l(z)$ можно обобщить над кольцом *P(z),* если конечное кольцо $P_l(z)$ содержит корень *d*-ой степени из единицы и *d* имеет мультипликативный обратный элемент d^*, такой что справедливо

$$d^* d = p^v - 1. \quad (3)$$

Представленная математическая модель цифровой обработки сигналов использует модулярный полиномиальный код. При этом вычисления организуются параллельно, помодульно и независимо друг от друга, т.е. для суммы, разности и произведения двух полиномов $A(z)$ и $B(z)$, имеющих соответственно модулярные коды $(\alpha_1(z), \alpha_2(z), ..., \alpha_n(z))$ и $(\beta_1(z), \beta_2(z), ..., \beta_n(z))$ справедливы соотношения при *i=1,...,n* [6–8]:

$$\left| A(z) \otimes B(z) \right|_{p(z)}^{+} = \left| \alpha_i(z) \otimes \beta_i(z) \right|_{p_i(z)}^{+}, \quad (4)$$

где $\otimes$ – операции сложения, вычитания и умножения в поле Галуа.

Тогда ортогональное преобразование сигнала и ему обратное определяются

$$\left(X_1(l), ..., X_n(l) \right) = \left(\sum_{j==0}^{d-1} x_1(j)\beta_1^{jl}, ..., \sum_{j=0}^{d-1} x_n(j)\beta_n^{jl} \right), \quad (5)$$

$$\left(x_1(j), ..., x_n(j) \right) = \left(d^* \sum_{l==0}^{d-1} X_1(l)\beta_1^{-jl}, ..., d^* \sum_{l=0}^{d-1} X_n(l)\beta_n^{-jl} \right). \quad (6)$$

При этом справедливо

$$\begin{aligned} &x_i(j) \equiv x(j) \bmod p_i(z); \; \beta_i^{\pm jl} \equiv \beta^{\pm jl} \bmod p_i(z); \\ &X_i(l) \equiv X(l) \bmod p_i(z). \end{aligned} \quad (7)$$

Приравнивая соответствующие координаты, получаем *n* пар прямого преобразования

$$\begin{cases} X_1(l) = \sum_{j=0}^{d-1} x_1(j)\beta_1^{jl} \bmod p_1(z); \\ \vdots \\ X_n(l) = \sum_{j=0}^{d-1} x_n(j)\beta_n^{jl} \bmod p_n(z), \end{cases} \quad (8)$$

и *n* пар обратного преобразования

$$\begin{cases} x_1(j) = d^* \sum_{l=0}^{d-1} X_1(l)\beta_1^{-jl} \bmod p_1(z); \\ \vdots \\ x_n(j) = d^* \sum_{l=0}^{d-1} X_n(l)\beta_n^{-jl} \bmod p_n(z). \end{cases} \quad (9)$$

Применение выражений (8) и (9) позволяет свести вычисление ортогональных преобразований сигналов в поле Галуа над кольцом *P(z)* к *n* независимым вычислениям, проводимым по модулям $p_i(z)$ кода МПК. Повысить скорость обработки сигналов можно за счет перехода к быстрым алгоритмам, которые используют матрицы меньшей размерности. Так для полинома третьей степени $p(z) = z^3 + z + 1$ *(deg p(z) = 3)* существует 7-точечное ортогональное преобразование. В этом случае используется матрица поворачивающих коэффициентов размером 7×7. Применение быстрого алгоритма ортогонального преобразования по модулю *p(z)*, позволяет осуществить эту процедуру на основе использования 3 матриц размером 2×2.

При этом применение модулярного полиномиального кода позволяет не только повысить скорость обработки данных, но и обеспечить восстановить искаженные результаты, которые возникают из-за отказов вычислительного устройства ЦОС [8, 10].

Если на диапазон возможного изменения кодируемого множества полиномов наложить ограничения, то есть выбрать *k* из *n* оснований МПК ($k < n$), то это позволит осуществить разбиение полного диапазона *P(z)* расширенного поля Галуа $GF(p^v)$ на два непересекающихся подмножества. Первое подмножество называется рабочим диапазоном

$$P_{раб}(z) = \prod_{i=1}^{k} p_i(z), \quad (10)$$

Второе подмножество $GF(p^v)$, определяемое произведением $r = n - k$ контрольных модулей

$$P_{конт}(z) = \prod_{i=k+1}^{k+r} p_i(z). \quad (11)$$

Многочлен $A(z)$ с коэффициентами из поля $GF(p)$ будет считаться разрешенным, в том и только том случае, если $\deg A(z) < \deg P_{раб}(z)$. В противном случае $A(z)$, представленный к МПК, считается ошибочным.

Отсутствие взаимосвязи между вычислительными трактами процессоров МПК не позволяет ошибкам перемещаться по другим основаниям. При этом изменение кратности ошибки не приводит к размножению ошибки как между разрядами внутри основания, так и от одного основания к другому.

В работе [10] проведены исследования корректирующих способностей модулярных полиномиальных кодов. Как показали исследования, для исправления однократной ошибки необходимо в состав упорядоченного МПК, для которого справедливо $\deg p_1(z) \le \deg p_2(z) \ldots \le \deg p_k(z)$, ввести два контрольных оснований $p_{k+1}(z)$ и $p_{k+2}(z)$, удовлетворяющих условию

$$\deg p_{k-1}(z) + \deg p_k(z) \le \deg p_{k+1}(z) + \deg p_{k+2}(z), \quad (12)$$

Пусть ошибка произошла по модулю $p_i(z)$. В этом случае ошибка изменяет значение остатка $\alpha_i(z)$ на величину $\Delta\alpha_i(z)$, так, что получается новое значение $\alpha_i^*(z) = \alpha_i(z) + \Delta\alpha_i(z)$. При этом правильный полином

$$A(z) = (\alpha_1(z), \ldots, \alpha_i(z), \ldots, \alpha_{k+2}(z)),$$

принадлежащий рабочему диапазону, преобразуется в запрещенный полином $A^*(z) = (\alpha_1(z), \ldots, \alpha_i^*(z), \ldots \alpha_{k+2}(z))$, лежащий вне рабочего диапазона. Таким образом, зная номер интервала, куда попал искаженный полином $A^*(z)$, можно определить основание, по которому произошла ошибка, а также ее глубину этой ошибки.

Согласно китайской теореме об остатках, используемой для преобразования из модулярного кода в позиционный код, значение ошибочного полинома $A^*(z)$ в этом случае определяется выражением

$$A^*(z) = \sum_{i=1}^{k+2} \alpha_i(z) B_i(z) \bmod P(z) = A(z) + \left| \Delta\alpha_j(z) B_j(z) \right|^+_{P_{пол}(z)} \quad (13)$$

где – $B_i(z)$ – ортогональный базис i-го основания МПК.

Анализ выражения (13) показывает, что местоположение ошибочного полинома $A^*(z)$ относительно рабочего диапазона $P_{раб}(z)$ определяется величиной второго слагаемого.

Данное свойство модулярных кодов и предопределило повышенный интерес разработчиков к позиционной характеристике – интервальный номер полинома $l(z)$ [10]. Процесс определения данной характеристики осуществляется согласно выражения

$$l_{инт}(z) = \left[A(z) / P_{раб}(z) \right]. \quad (14)$$

Несмотря на то, что процедура (14) относится к немодульным, ее сводят к совокупности модульных операций. В работе [6] представлено устройство, осуществляющее обнаружение и коррекцию ошибки в модулярном коде на основе вычисления интервального номера. В основу данного алгоритма положено свойство подобия ортогональных базисов полной, содержащей контрольные основания, и безизбыточной системы МПК, согласно которому

$$B_i^*(z) \equiv B_i(z) \bmod P_{раб}(z), \quad (15)$$

где $B_i^*(z)$ и $B_i(z)$ – ортогональные базисы безизбыточной и полной системы.

Тогда согласно (15) справедливо

$$B_i(z) = R_i(z) \cdot P_{раб}(z) + B_i^*(z), \quad (16)$$

где $R_i(z) = \left\lfloor B_i(z) / P_{раб}(z) \right\rfloor$.

Подставив последнее равенство в выражение (13) получаем

$$l_{инт}(z) = \sum_{i=1}^{k+2} \alpha_i(z) (R_i(z) P_{раб}(z) + B_i^*(z)) + K(z) P_{полн}(z)) / P_{раб}(z). \quad (17)$$

где $K(z)$ – ранг полной системы оснований МПК.

Проведя упрощения, имеем

$$l_{инт}(z)=\sum_{i=1}^{k+2}\alpha_i(z)R_i(z)+\left[\sum_{j=1}^{k}\alpha_j(z)B_j^*(z)\Big/P_{раб}(z)\right]+K(z)P_{полн}(z))/P_{раб}(z). \quad (18)$$

Так как множество значений интервального номера $l_{инт}(z)$ представляет собой кольцо по модулю $P_{конт}(z)=\prod_{i=k+1}^{k+2}p_i(z)$, то выражение (18) имеет вид

$$l_{инт}(z)=\left|\sum_{i=1}^{k+r}\alpha_i(z)R_i(z)+K^*(z)\right|^{+}_{P_{конт}(z)}, \quad (18)$$

где $K^*(z)$ – ранг безизбыточной системы определяется выражением

$$K^*(z)=\left[\sum_{j=1}^{k}\alpha_j(z)B_j^*(z)\Big/P_{раб}(z)\right]. \quad (19)$$

Следовательно, если $l_{инт}(z)=0$, то исходный полином $A(z)$ лежит внутри рабочего диапазона и не является запрещенным. В противном случае $A(z)$ – ошибочная комбинация. Пусть задан модулярный полиномиальный код, который имеет рабочие основания $p_1(z)=z+1;\ p_2(z)=z^2+z+1;\ p_3(z)=z^4+z^3+z^2+z+1$. В качестве контрольных оснований используются полиномы $p_4(z)=z^4+z^3+1;\ p_5(z)=z^4+z+1$, которые удовлетворяют условию (12). Тогда рабочий диапазон равен $P_{раб}(z)=\prod_{i=1}^{3}p_i(z)=z^7+z^6+z^5+z^2+z+1$. В табл. 1 представлены номера интервалов, в которые попадают ошибочные полиномы $A_l^*(z)$,при возникновении однократной ошибки по основаниям МПК

Таблица 1

Распределение однократных ошибок кода МПК

Основание ПСКВ	Глубина $\Delta\alpha_i(z)$	Интервал, представленный в полиномиальной форме
$p_1(z)=z+1$	1	$z^7+z^4+z^2+z$
$p_2(z)=z^2+z+1$	1	$z^7+z^5+z^2+z+1$
	z	$z^7+z^6+z^5+z^4+z^2$
$p_3(z)=z^4+z^3+z^2+z+1$	1	$z^7+z^4+z^3+z+1$
	z	z^7+z^3+z+1
	z^2	z^7+z^5
	z^3	$z^7+z^6+z^5+z^4+z^3+z+1$
$p_4(z)=z^4+z^3+1$	1	$z^7+z^4+z^3$
	z	z^7+z^3+z+1
	z^2	$z^7+z^5+z^3+z^2$
	z^3	$z^7+z^6+z^5+1$
$p_5(z)=z^4+z+1$	1	z^5+z^4+z
	z	$z^6+z^5+z^2$
	z^2	$z^7+z^6+z^3$
	z^3	z^5+z^3+z+1

Анализ таблицы показывает, что ошибка переводит разрешенную модулярную комбинацию в соответствующий интервал полного диапазона. Очевидно, что использование двух контрольных оснований, удовлетворяющих (12), позволяет по

величине $l_{инт}(z)$ определить местоположение и глубину $\Delta\alpha_i(z)$ ошибки. При этом такой избыточный модулярный код способен исправить более 90 процентов двукратных ошибок.

Заключение. В работе показана целесообразность использования математической модели цифровой обработки сигналов, реализуемой в кольце полиномов. Применение модулярного полиномиального кода позволяет повысить точность и скорость обработки сигналов за счет выполнения арифметических операций над малоразрядными остатками. Кроме этого использование модулярного полиномиального кода позволяет обеспечить коррекцию искаженного результата в условиях воздействия помех при передаче и отказа оборудования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Rohde & Schwarz*. R&S FSQ-K96 OFDM Vector Signal Analysis with the R&S FSQ Signal Analyzer. Product Brochure, V. 1.00, March 2008
2. *Yong Soo Cho, Jaekwon Kim, Won, Young, Chung G. Kang* MIMO-OFDM Wireless Communications with MATLAB, – WILEY, 2010.
3. *Farinas Edalat* Sub-carrier Adaptive Modulashion and Coding in OFDM, LAMBERT, 2010.
4. *Чипига А.Ф., Шевченко В.А., Сенокосова А.В., Дагаев Э.Х.* Математическая модель трансионосферного канала с учетом поглощения и многолучевости принимаемого сигнала // Вестник Северо-Кавказского государственного технического университета. – 2011. – № 1. – С. 23-28.
5. *Катков К.А., Пашинцев В.П., Гахов Р.П.* Адаптивный алгоритм определения вектора пространственно-временных координат // Вопросы радиоэлектроники. – 2013. – Вып. 1. – С. 138-150.
6. *Калмыков И.А., Воронкин Р.А, Резеньков Д.Н., Емарлукова Я.В.* Генетические алгоритмы в системах цифровой обработки сигналов // Нейрокомпьютеры: разработка и применение. – 2011. – Вып. 5. – С. 20-27.
7. *Калмыков, И.А., Дагаева О.И.* Применение системы остаточных классов для формирования псевдослучайной функции повышенной эффективности // Вестник Северо-Кавказского технического университета. – 2012. – Вып. 3. – С. 26-30
8. *Калмыков И.А., Зиновьев А.В., Емарлукова Я.В.* Высокоскоростные систолические отказоустойчивые процессоры цифровой обработки сигналов для инфокоммуникационных систем // Инфокоммуникационные технологии. – 2009. – Т. 7, № 2. – С. 31-37.
9. *Hosseinzadeh M., Navi K., Gorgin S.* A New Moduli Set for Residue Number System. Electrical Engineering, 2007. ICEE'07. International Conference on. 11–12 April 2007. – P. 1-6.
10. *Калмыков И.А.* Математические модели нейросетевых отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов / Под ред. Н.И. Червякова – М.: Физматлит, 2005. – 276 с.

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.: 88652731380, 89034163533; кафедра информационной безопасности автоматизированных систем; д.т.н.; профессор.

Саркисов Артем Брониславович – e-mail: zik@ncstu.ru; 355000 г. Ставрополь, пр. Кулакова, 27, кв. 38; тел.: 88652956546; кафедра информационной безопасности автоматизированных систем; аспирант.

Макарова Алена Васильевна – e-mail: alyonchikMav@yandex.ru; 355000 г. Ставрополь, ул. Ленина, 445; тел.: 89187647533; кафедра информационной безопасности автоматизированных систем; аспирантка.

Kalmykov Igor Anatolyevich – Institute of Information Technologies and Telecommunications, North-Caucasus Federal University, Stavropol; e-mail: kia762@yandex.ru; 92, Shpakovskaya street, k. 1, fl. 28, Stavropol, 355000, Russia; phones: +78652731380, +79034163533; the department of information security of automated systems; dr. of eng. sc.; professor.

Sarkisov Artyom Bronislavovich – e-mail: zik@ncstu.ru; 27, pr. Kulakova, fl. 38, Stavropol, 355000, Russia; phone: +78652956546; the department of information security of automated systems; postgraduate student.

Makarova Alyona Vasil'evna – e-mail: alyonchikMav@yandex.ru; 445, Lenina street, Stavropol, 355000, Russia; phone: +79187647533; the department of information security of automated systems; postgraduate student.

УДК 004.056:061.68

В.М. Федоров, Д.П. Рублев, Е.М. Панченко

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ ПО ВИБРОАКУСТИЧЕСКИМ ШУМАМ, ВОЗНИКАЮЩИМ ПРИ НАБОРЕ ПРОИЗВОЛЬНОГО ТЕКСТА НА КЛАВИАТУРЕ*

Рассмотрена проблема идентификация пользователя по виброакустическому сигналу, возникающему при наборе произвольного текста на клавиатуре. Для повышения точности идентификации пользователя по виброакустическим шумам разработан метод удаления пауз удалялись паузы между нажатиями/отпускания клавиш клавиатуры. Была сформирована обучающая выборка виброакустических шумов возникающих при нажатии/отпускании клавиш и виброакустических шумов присутствующих в паузах при набирании текста. Полученные выборки были использованы как обучающие данные для обучения нейронной сети. Для выделения участков с паузами виброакустические сигналы разбивались на интервалы длиной 1024 точек с перекрытием на половине интервала, в случае принадлежности участка к паузе, данный участок удалялся. Рассмотрены и произведен выбор устойчивых признаков, характеризующих личность пользователя: коэффициенты Фурье преобразования, кепстр, коэффициенты линейного предсказания. Рассмотрены методы идентификации пользователя на основе статистических параметров, гауссовские смешанные модели и нейронных сетей. Показана возможность идентификации пользователя по виброакустическим шумам, возникающим при наборе данных на клавиатуре, оценена вероятность правильной распознавания пользователя для созданной базы виброакустических сигналов пользователей.

Виброакустический сигнал; дискретное Фурье преобразование; кепстральные коэффициенты; нейронные сети; коэффициенты линейного предсказания; гауссовские смешанные модели; идентификация; контроль доступа.

V.M. Fedorov, E.M. Panchenko, D.P. Rublev

USER IDENTIFICATION BASED ON VIBROACOUSTIC NOISES ORIGINATED FROM ARBITRARY TEXT TYPING

In presented work the user identification task based on vibroacoustic signal originated from typed arbitrary text is reviewed. To increase identification accuracy the method of keypresses/releases pauses removal was developed. A training sets consisting of vibroacoustics signals of keypresses/releases and vibroacoustics noises in pauses has been developed. Obtained sets were used as training data for neural net. Pauses detection was done in running window with 1024 samples length overlapped by ½ of its length. If window fragment was detected as belonging to pause segment, this fragment was removed. Features for detection user identity were considered and stable set of features was selected, namely: Fourier transform coefficients, cepstral coefficients and linear prediction coefficients. User identification methods based on statistical parame-

* Работа выполнена при поддержке гранта РФФИ №12-07-00674-а.