УДК 681.142.7

ТЕОРЕТИКО-ПРИКЛАДНЫЕ АСПЕКТЫ ОРТОГОНАЛЬНОГО КОДИРОВАНИЯ В СЕТЕВЫХ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЯХ

В.Н. Бурков[1], В.Ф. Макаров[2]

[1] Институт проблем управления
им. В.А. Трапезникова
[2] Академия управления МВД России

В статье рассматриваются вопросы формирования нового модифицированного множества ортогональных сигналов, математическими моделями которых является модифицированное множество кусочно-постоянных ортогональных функций Радемахера и Уолша. Приведена методика формирования множества ортогональных сигналов для передачи данных по каналам связи и обработки сложного составного многоуровневого суммарного сигнала, форма которого отображает состояние параллельного интерфейса вычислительного комплекса, и его обработку псевдокорреляционными устройствами приемника.

Ключевые слова: *ортогональные функции Уолша и Радемахера, модификация ортогональных сигналов, суммирование по модулю два, псевдокорреляционная обработка суммарного ортогонального множества, устойчивость к несанкционированному распознаванию, уплотнение и разделение сигналов по форме.*

THEORETICAL AND PRACTICAL ASPECTS OF ORTHOGONAL ENCODING IN COMPUTER NETWORKING TECHNOLOGIES

V.N. Burkov, V.F. Makarov

In article questions of formation of the new modified set of the orthogonal signals which mathematical models is the modified set of piecewise and continuous orthogonal functions of Rademakher and Walsh are considered. The technique of formation of a set of orthogonal signals for data transmission on communication channels and processings of the difficult compound multilevel total signal which form displays a condition of the parallel interface of the computer system, and its processing by pseudo-correlation devices of the receiver is given.

Keywords: *Walsh and Rademakher's orthogonal functions, modification of orthogonal signals, summation on the module two, pseudo-correlation processing of a total orthogonal set, resistance to unauthorized recognition, consolidation and division of signals in a form.*

Вопросам построения надежных цифровых систем передачи и обработки данных с использованием методов помехоустойчивого и помехозащищенного кодирования, устойчивых к несанкционированным воздействиям, уделялось и уделяется значительное внимание как у нас в стране, так и за рубежом. В настоящее время достаточно большой интерес вызывают вопросы помехоустойчивого кодирования с использованием ортогональных кодов, математическими моделями которых являются множества ортогональных функций и полиномов, что нашло свое отражение в разработках Л.М. Гольденберга [1], Л.А. Залманзона [2], С. Качмаж [3], В.В. Сюзева [14], Х. Хармута [15] и др.

На сегодняшний день разработан стандарт цифровой системы подвижной радиосвязи с кодовым разделением каналов (CDMA компании Hutchison Telephone), которая построена на основе базовых станций SC 9600 и коммутационной станции EMX 2500 (Motorola), а также стандарт цифрового телевидения DVB-T, использующих многоуровневые кусочно-постоянные ортогональные сигналы.

Однако необходимо отметить, что авторами данной статьи, начиная с 1971 г. и до наших дней велись и ведутся разработки и получены авторские свидетельства и патенты на изобретения (7 авторских свидетельств и 4 патента на изобретения) по проблемам построения систем передачи информации (телеметрической, речевой, телевизионной, компьютерной) на основе средств и методов построения канальных сигналов, математическими моделями которых являются множество кусочно-постоянных ортогональных функций Уолша, с последующей их обработ-

кой приемными корреляционными устройствами [9–14].

На применение ортогональных кодов как одного из наиболее эффективных методов повышения достоверности обработки информации было указано в работах академика В.А. Котельникова [4]. Основным достоинством методов помехоустойчивого кодирования является обнаружение и исправление ошибок, возникающих за счет воздействия помех в кодовых комбинациях. Эта возможность обнаружения и исправления ошибок достигается за счет введения избыточности при построении кодовых таблиц. Причем ошибки могут обнаруживаться и исправляться только лишь в пределах, ограниченных корректирующей способностью кода.

Одним из методов уплотнения и разделения канальных сигналов и отдельных элементов ортогональных кодов, позволяющих не только устранять избыточность, но и обеспечивать высокую достоверность обработки информации является применение ортогональных кодов с последующей обработкой их приемными корреляционными устройствами. По своей структуре такие сигналы относятся к сложным составным сигналам, база которых много больше единицы (B=F×T>>1) и которые являются разновидностью шумоподобных сигналов.

При построении систем теледоступа к вычислительным ресурсам, использующим ортогональные коды, математическими элементами которых являются множества различных ортогональных кусочно-постоянных или непрерывных ортогональных функций или полиномов, необходимо создать базис первообразных ортогональных функций или полиномов. Известно, что при построении многоканальных систем передачи данных с уплотнением и разделением канальных сигналов по форме применяются различные ортогональные кодовые последовательности, построенные на основе ортогональных функций или полиномов Лежандра, Чебышева, Лагерра, Эрмита, Якоби, Бесселя, Гегенбауэра, Радемахера, Хаара, Уолша [3]. Из всех перечисленных функций и полиномов необходимо выбрать только те, которые наиболее эффективны для образования канальных сигналов или отдельных элементов кодовых комбинаций.

Так, полиномы Лагерра и Эрмита ортогональны на интервале -∞ ... +∞ и 0 ...+∞ и ограничение периода передачи сообщений связано с нарушением ортогональности, а, следовательно, и с появлением взаимовлияния канальных сигналов.

Функции Гегенбауэра и Якоби удовлетворяют условию конечных пределов ортогональности, но их техническая реализация связана со значительными сложностями. Функции Бесселя первого и второго родов не полностью ортогональны и их применение также связано с появлением ошибок за счет взаимовлияния.

Наиболее приемлемыми функциями в качестве сигналообразующих являются ортогональные полиномы Чебышева и Лежандра и ортогональные функции Радемахера и Уолша. Однако техническая и программная реализация сигналов, математическими моделями которых являются ортогональные полиномы Чебышева и Лежандра, также затруднительна из-за применения в передающих и приемных устройствах сложных аналоговых устройств умножения [6].

Наиболее приемлемыми для построения ортогональных сигналов и ортогональных кодов являются ортогональные функции Радемахера и Уолша [4]. Однако при выборе тех или иных ортогональных функций и полиномов в качестве математических моделей ортогональных сигналов и ортогональных кодов при построении систем теледоступа к вычислительным ресурсам необходимо руководствоваться не только степенью сложности их реализации, но также и степенью подверженности таких сигналов различному виду помех, а также к несанкционированному восприятию и распознаванию.

Внешними возмущающими воздействиями являются импульсные и флуктуационные помехи, помехи типа «пакет», помехи, сосредоточенные по спектру или по времени. Наиболее устойчивыми сигналами к воздействию помех будут такие сигналы, у которых степень соответствия с помехами будет минимальной. Так, для случая импульсных помех, преобладающих в каналах теледоступа, такую оценку можно производить по коэффициентам аппроксимации реакции линии связи на ударное возбуждение от импульсных помех. В этом случае реакция линии связи на ударное возбуждение может быть выражена линейной комбинацией взаимно ортогональных функций, если последние образуют полный базис.

Для тех функций, у которых при одинаковом числе членов суммы аппроксимирующего ряда коэффициенты аппроксимации будут минимальными, соответствие между функциями, описывающими информационные сигналы и помехи, также будет минимальным. Следовательно, и сигналы, описываемые этими ортогональными функциями, будут наиболее устойчивыми к разрушающему воздействию помех:

$$\beta = \frac{\int_0^T U_n(t) * U_c(t)dt}{\int_o^T U_c^2(t)dt}, \qquad (1)$$

где: $Un(t)$ – система ортогональных функций, описывающих помеху; $Uc(t)$ – система ортогональных функций, описывающих полезный сигнал.

Анализ существующих методов организации системы теледоступа к вычислительным ресурсам показал, что они используют, в основном, временное уплотнение и разделение канальных сигналов, которое

по достоверности проигрывает иным способам многоканальной передачи данных. В этом плане наиболее перспективным является организация теледоступа с уплотнением и разделением канальных сигналов по форме, в которой в качестве канальных сигналов используются ортогональные коды, построенные на основе ортогональных функций Уолша, в совокупности с оптимальной обработкой их в приемных корреляционных устройствах.

В рассматриваемой системе для построения канальных кодообразующих сигналов используется обобщенная полная система ортогональных кусочно-постоянных функций Уолша. Такой подход требует новых качественных изменений в построении общей теории связи, основанной на синусно-косинусных функциях и цифровых методах обработки информации. В этом случае описание методов обработки сигналов происходит не в частотно-временной, а в функционально-временной плоскости.

Следовательно, любая последовательность ортогональных сигналов, построенных на полной системе ортогональных функций, занимает конечную часть функционально-временной плоскости.

Под полной ортонормированной системой функций понимается такая система, в которой для любой функции $F_i(t)$ предел квадратично интегрируемой разности устремляется к нулю. Для такой системы неравенство Бесселя $\sum_{k=1}^{\infty} F_m^2 \le \|a\|^2$ в предельном переходе обращается в равенство Парсеваля. Подобное представление позволяет оценивать в физическом смысле энергию несинусоидальных колебаний как сумму энергий отдельных спектральных составляющих:

$$\int_0^T F^2(t)\,dt = \sum_{k=1}^{\infty} (a_k^2 + b_k^2). \qquad (2)$$

Такой подход позволяет вычислять значения сигналов на выходах отдельных корреляционных устройств многоканальных систем передачи данных с разделением каналов по форме, канальные сигналы которых построены на основе несинусоидальных сложных составных ортогональных функций или полиномов [4].

Построение каналообразующей аппаратуры компьютеризированных комплексов, защита преобразуемых и передаваемых данных с использованием в качестве элементов кодовых комбинаций ортогональных сигналов, построенных на основе множеств ортогональных функций или полиномов, до настоящего времени не получило широкого распространения из-за относительно малой степени изученности по сравнению с классическими методами обработки данных.

В данной статье рассматриваются вопросы организации системы передачи и защиты данных в компьютерных технологиях с использованием методов уплотнения и разделения элементов кодовых комбинаций по форме, математическими моделями которых являются ортогональные функции Уолша, относящиеся ко множеству ортонормированных кусочно-постоянных ортогональных функций.

Следует отметить, что система $\{f(j, x)\}$ действительных и ненулевых функций называется ортогональной на конечном интервале $x_0 \le x \le x_1$, если выполняются следующие условия:

$$\int_{x_0}^{x_1} f(j,x)\cdot f(k,x) = x_j \cdot \delta_{jk}, \quad \delta_{jk} = \begin{cases} 1, & j = k \\ 0, & j \ne k \end{cases} \qquad (3)$$

Эти условия ортогональности определены в метрике гильбертова пространства. В евклидовом пространстве условие ортогональности определяется как:

$f(j, x) \times f(k, x) = f(j, x) \times f(k, x) \times \cos\varphi = xj\eth jk$

$$\delta_{jk} = \begin{cases} 1, & \varphi = 0^\circ \\ 0, & \varphi = 90^\circ \end{cases}. \qquad (4)$$

Из выражений (2, 3) следует, что векторы, описывающие элементы сигналов или кодовых комбинаций являются ортогональными, если их скалярное произведение равно 1 в случае полного их совпадения и 0 в противном случае.

В исследованиях, проведенных Уолшем, показана возможность формирования полной системы ортогональных кусочно-постоянных функций на основе базисных ортогональных функций Радемахера, являющихся подмножеством полного кусочно-постоянного множества ортогональных функций Уолша.

В такой системе базовыми ортогональными функциями Радемахера являются функции вида $M_r = \{Y_1, Y_2, Y_4, Y_8, Y_{16}, \ldots Y2^n\}$. Полная система ортогональных функций Уолша формируется из базисной ортонормированной системы кусочно-постоянных функций Радемахера путем их алгебраического перемножения, например из ортогональных функций Радемахера Y_1 и Y_2 функция Уолша Y_3 определится как $Y_3=Y_1\times Y_2$. Каждые последующие производные функции Уолша образуются согласно алгоритму:

$$Y_5=Y_1\times Y_4;\ Y_6=Y_2\times Y_4;\ Y_7=Y_1\times Y_2\times Y_4;\ Y_9=Y_1\times Y_8;\ldots;$$
$$Y_{15}=Y_1\times Y_2\times Y_4\times Y_8. \qquad (5)$$

При определении необходимого и достаточного числа ортогональных функций Уолша для построения отдельных элементов ортогональных кодов в системах защиты и передачи данных необходимо выявить максимальный нижний предел номера базисной функции Радемахера sup Kj. После чего определяются и сами

базисные функции выбранного подмножества, из которых на основе перемножения формируется полная система ортогонального подмножества Уолша [8]. Порядковый номер каждой такой функции определяется в соответствии со следующей формулой:

$$m = \sup K_j + \sum_{j=1}^{2^{n-1}} K_j, \qquad (6)$$

где m – порядковый номер производной функции Уолша; Kj – номера базисных образующих функций Радемахера.

В свою очередь, порядковый номер производной функции Уолша определяет ее структурный состав, т.е. подмножество образующих функций Радемахера.

В общем виде алгоритм образования сигналообразующих кусочно-постоянных ортогональных функций Уолша определится как

$$Y_m = Y_{\sup Kj} \times \prod_{j=1}^{2^n} Y k_j \{ \forall Y_m, \sup K_j + \sum_{j=1}^{2^n} K_j \}. \qquad (7)$$

В соответствии с формулой (5) на рис. 1 представлен фрагмент множества ортогональных кусочно-постоянных ортонормированных функций Уолша для построения кодовых ортогональных кодовых комбинаций, состоящих из 64 элементов ортогональных кодов, отображенных в кусочно-постоянном ортогональном множестве Уолша.

При этом необходимо отметить, что эта система отличается от классической системы ортогональных функций Уолша. Авторам статьи удалось получить модернизированное множество кусочно-постоянных функций Уолша в том отображении, при котором все сложные составные элементы отдельных функций Уолша строго фазированы, т.е. начинаются с одной фазы, что имеет существенное значение, как при технической, так и программной реализации полной совокупности кодовых ортогональных сигналов в системах теледоступа к вычислительным ресурсам. Это преимущество определяется, прежде всего, тем, что не требуется введение специальных блоков распознавания начальной фазы, как отдельных канальных сигналов, так и сложного составного суммарного сигнала, форма которого будет определять текущее состояние параллельного интерфейса вычислительного комплекса.

Как видно из рис. 1, полная система ортогональных функций Уолша состоит из четных и нечетных функций, принимающих на всем периоде значения «+1» или «-1». Однако при этом необходимо осуществить проверку полученных ортогональных функций на отсутствие нарушения их ортогональности. Проверка полученных и построенных функций Уолша показывает, что, какая бы комбинация не была взята, условие ортогональности полностью сохраняется. Последнее утверждение позволяет сохранить сепарабельность построенного множества, а следовательно осуществить распознавание и выделение каждого элемента приведенного множества кусочно-постоянных ортогональных функций.

Пример отображения образования подмножества Уолша из базисных функций Радемахера представлен в виде графа (рис. 2), на котором прослеживается алгоритм формирования производных функций на основе базисных функций Радемахера (для случая Y_1; Y_2; Y_4; Y_8), причем необходимо отметить, что номер каждой производной функции Уолша определяется суммой номеров функций Радемахера, входящих в рассматриваемый узел.

Преобразованный граф характерен тем, что каждая последующая функция образуется в результате перемножения одной из базовых и производных

Y1=-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1+1+1+1+
+ 1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1
Y2=-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1
-1 -1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1
Y3=+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1
-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1+1
……..
Y63=+1-1-1+1-1+1+1-1-1+1+1-1+1-1-1+1-1+1+1-1+1-1-1+1+1-1-1+1+1-1+1+1-1-1+1+1-1+1-1-
1+1+1-1-1+1-1+1+1-1+1-1-1+1-1+1+1-1-1+1+1-1+1+1-1-1+1

РИС. 1.
Фрагмент 63 ортогональных функций Уолша в двоичной форме

функций или двух базовых функций, т.е. в этом случае каждый узел графа имеет только два входа. Полученное условие является весьма важным при технической реализации генератора ортогональных колебаний, т.к. в этом случае его построение ориентировано на применение двухвходовых схем совпадения в устройствах умножения ортогональных сигналов.

Последнее преобразование также важно и при программной реализации генератора ортогональных колебаний, математическими моделями которых является множество кусочно-постоянных ортогональных функций Уолша, т.к. в этом случае производится поэлементное умножение только лишь двух функций, что резко сокращает время формирования разрешенного ортогонального множества кодовых элементов.

При последовательном построении множества ортонормированных функций Уолша каждая последующая функция строится по следующему алгоритму:

1. Строятся две первые ортогональные функции Радемахера Y_1 и Y_2.

2. Путем поэлементного их перемножения определяется и строится функция Y_3.

3. Вводится еще одна функция Радемахера Y_4.

4. Путем поэлементного перемножения функций Y_1 и Y_4, Y_2 и Y_4, Y_3 и Y_4 строятся функции Y_5, Y_6, Y_7.

Этот процесс дополнения множества Уолша продолжается до получения необходимого количества ортонормированных функций для построения множества кодообразующих ортогональных сигналов или элементов ортонормированного кода Уолша.

Производится временное закрепление элементов выбранного ортогонального множества за элементами байта Windows-кода в соответствии с таблицей кодирования, представленной $Y_k \to W_k$.

Такое закрепление динамично и может изменяться при каждом сеансе передачи данных. В силу того, что ортогональные сигналы, являющиеся моделями ортогональных функций Уолша, параллельны во времени, возможна передача не последовательности битов Windows-кода, а сложного составного многоуровневого суммарного сигнала, состоящего из множества ортогональных сигналов Уолша и отображающего состояние параллельного интерфейса вычислительного комплекса в едином временном интервале – T.

Последнее дает возможность формирования на кодирующем устройстве сложного составного многоуровневого сигнала, несущего информацию о кванте передаваемых данных. Таким семантическим квантом может быть не один, а несколько символов естественного алфавита.

В рассматриваемом примере таким семантическим квантом является слово, часть слова, фраза, состоящие из семи семантических элементов (букв). Для отображения любой семизначной комбинации естественных символов кириллицы, цифрового алфавита и знаков пунктуации, интерпретируемых в Windows-кодах потребуется порядка 64 ортогональных сигналов Уолша.

Причем изначально любые восемь функций Уолша закрепляются за разрядами восьмиэлементного Windows-кода, отображающими первый символ естественного алфавита, затем из оставшихся ортогональных сигналов восемь закрепляются за разрядами второго символа кодируемого текста и т.д. В результате такого преобразования все семь символов кодируемого текста отображаются на множестве ортогональных функций Уолша

$$\forall x_i \in X \to \{a_w\}|8 \to \{y_i \in Y\}|64. \qquad (8)$$

Такое отображение производится с помощью оператора преобразования, устанавливающего правила соответствия между элементами Windows-кодов и элементами множества ортогональных функций Уолша. После установления соответствия между множеством элементов байта Windows-кода, отображающих семантический символ естественного алфавита, и множеством ортогональных сигналов «Уолша» по

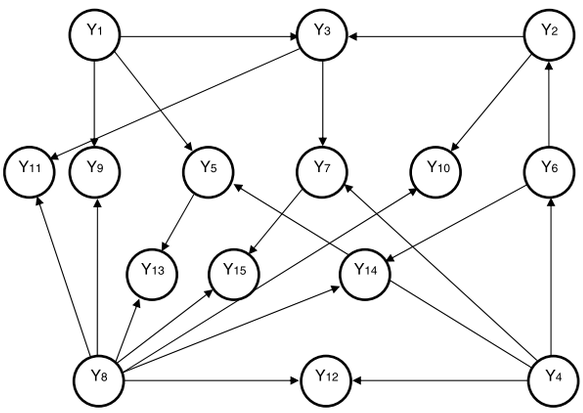

РИС. 2.
Пример преобразованного графа

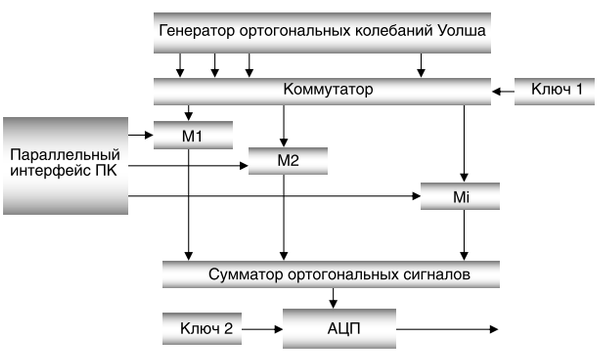

РИС. 3.
Структурная схема системы ортогонального кодирования

графику соответствий, который определяется задаваемой и динамически изменяемой таблицей преобразований, производится суммирование выбранных ортогональных сигналов. В результате такого преобразования формируется сложный составной суммарный многоуровневый сигнал, отображающий в текущий момент времени состояние параллельного интерфейса вычислительного комплекса. Структурная схема системы ортогонального кодирования представлена на рис. 3 [5, 6].

На диаграмме рис. 4 отображен сложный составной многоуровневый суммарный сигнал слова «Криптон», состоящий из 56 ортогональных сигналов Уолша (Y_1...Y_{56}).

3. Следующим шагом преобразования параллельного Windows-кода является отображение сложного составного многоуровневого сигнала выбранного ортогонального множества в двоичный код. Для осуществления такого преобразования формируется динамическая таблица преобразования, устанавливающая соответствие между отдельными уровнями суммарного многоуровневого сигнала и множеством двоичных кодовых комбинаций

В случае выбранного разрешенного ортогонального множества Уолша количество уровней суммарного сигнала, отображающего состояние параллельного интерфейса вычислительного комплекса, на рассматриваемом примере, составит 64 кванта.

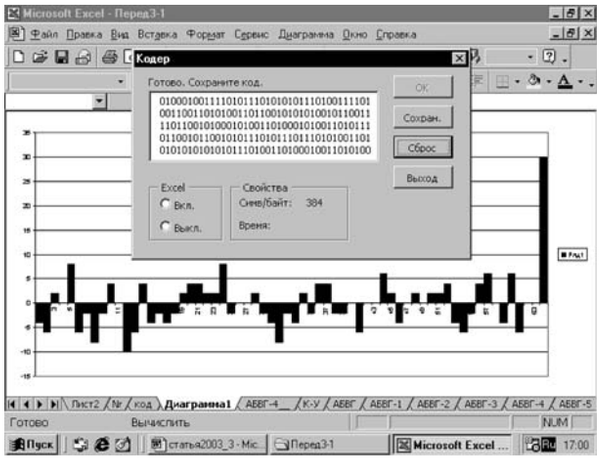

РИС. 4.

Отображение слова «Криптон» сложным составным многоуровневым сигналом, состоящим из 56 ортогональных сигналов «Уолша»

Литература

1. **Гольденберг Л.М., Матюшкин Б.Д. Поляк М.Н.** Цифровая обработка сигналов. М.: Радио и связь, 1990. 256 с.
2. **Залманзон Л.А.** Преобразование Фурье, Уолша, Хаара и их применение в управлении, связи и других областях. М.: Наука, 1989. 429 с.
3. **Качмаж С., Штейнгауз Г.** Теория ортогональных рядов. М.: Наука, 1958. 429 с.
4. **Котельников В.А.** Теория потенциальной помехоустойчивости. М.: Радио и Связь, 1956. 152 с.
5. **Макаров В.Ф.** Теоретические основы передачи и защиты информации в системах теледоступа к вычислительным ресурсам. М.: Академия управления МВД РФ, 1992. 224 с.
6. **Макаров В.Ф., Нечаев Д.Ю.** Методы защиты информационной инфраструктуры экономических систем. М.: РГТЭУ, 2011. 195 с.
7. **Макаров В.Ф.** Передача информации в компьютерных технологиях на основе ортогональных сигналов // Информационные системы и технологии, 2014. №2. С. 101–109.
8. **Макаров В.Ф., Нечаев Д.Ю.** Устранение избыточности в системах ортогонального кодирования // Безопасность информационных технологий. 2014. №2. С. 54–59.
9. **Макаров В.Ф. и др.** Устройство для приема телевизионных сигналов. Патент на изобретение № 2144741. Зарегистрирован в Государственном реестре изобретений РФ 20.01.2000.
10. **Макаров В.Ф. и др.** Устройство для передачи телевизионных сигналов. Патент на изобретение № 2131646. Зарегистрирован в Государственном реестре изобретений РФ 10.06.1999.
11. **Сюзев В.В.** Основы теории цифровой обработки сигналов. М.: РТСофт, 2014. 715 с.
12. **Хармут Х.** Теория секвентного анализа. Основы и применения. Пер. с англ. М.: Мир, 1980. 574 с.

Бурков Владимир Николаевич,
д.т.н., профессор, зав. лабораторией Института проблем управления им. В.А. Трапезникова РАН

117997, г. Москва, ул. Профсоюзная, д. 65,
тел.: +7 (495) 334-79-00

Макаров Валерий Федорович,
д.т.н., профессор кафедры информационных технологий управления Академии управления МВД России

117997, г. Москва, ул. З. и А. Космодемьянских, д. 8,
тел.: +7 (909) 657-35-48, e-mail: ovorta@mail.ru,