



**Макаров
Валерий Федорович,**

профессор кафедры информационных технологий управления органами внутренних дел Академии Управления МВД России, д.т.н., профессор, академик РАЕН по секции информатика и кибернетика

Вопросам построения надежных цифровых систем передачи и обработки данных с использованием методов помехоустойчивого и помехозащищенного кодирования, устойчивых к несанкционированным воздействиям, значительное внимание уделялось и уделяется 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 Гольденберга Л. М., Залманова Л. А., Качмаж С., Сюзева В. В., Хармута Х. и др.

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

Однако необходимо отметить, что автором данной статьи с 1971 года ведутся разработки и патенты на изобретения (7 авторских свидетельств и 4 патента на изобретения) по проблемам построения систем передачи информации (телеметрической, ре-

Методы ортогонального кодирования в сетевых компьютерных технологиях

чевой, телевизионной, компьютерной) на основе средств и методов построения канальных сигналов, математическими моделями которых является множество кусочно-постоянных ортогональных функций Уолша, с последующей их обработкой приемными корреляционными устройствами [7, 8, 9].

На применение ортогональных кодов как одного из наиболее эффективных методов повышения достоверности обработки информации было указано в работах академика В. А. Котельникова [2]. 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 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 ($B = F \cdot T \gg 1$) 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 [1]. 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 $-\infty \dots +\infty$ и $0 \dots +\infty$, и ограничение периода передачи сообщений связано с нарушением ортогональности, а следовательно, и с появлением взаимовлияния канальных сигналов.

Функции Гегенбауэра и Якоби соответствуют 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 [4].

Наиболее приемлемыми для построения ортогональных сигналов и ортогональных кодов являются ортогональные функции Радемахера и Уолша [2]. Однако при выборе тех или иных ортогональных функций и полиномов в качестве математических моделей ортогональных сигна-



лов 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. Важно плюс ко всему учитывать возможность несанкционированного восприятия и распознавания.

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, обладающих в каналах теледоступа, данного рода 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 будут минимальными. Следовательно, и сигналы, описываемые этими ортогональными функциями, будут наиболее устойчивыми к разрушающему воздействию помех.

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

Где: $U_n(t)$ — система ортогональных функций, описывающих помеху; $U_c(t)$ — 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 каналов сигналов, которое по достоверности проигрывает иным способам многоканальной передачи данных. В этом плане наиболее перспективным является организация теледоступа с уплотнением и разделением каналов сигналов по форме, в которой в качестве каналов сигналов используются ор-

тогональные 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 синусо-косинусных функциях и цифровых методах обработки информации. В этом случае описание методов обработки сигналов происходит не в частотно-временной плоскости, 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

$$\sum_{k=1}^{\infty} F_m^2 \leq \|a\|^2 \quad (2)$$

в предельном переходе обращается в равенство Парсеваля. Подобное представление позволяет оценивать в физическом смысле энергию несинусоидальных колебаний как сумму энергий отдельных спектральных составляющих:

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

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 [2].

Построение каналобразующей 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 $x_0 \leq x \leq x_1$, если выполняются следующие условия:

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

Эти условия ортогональности определены в метрике гильбертова пространства. В евклидовом пространстве условие ортогональности определяется как: $f(j, x) \times f(k, x) = f(j, x) \cdot f(k, x) \cdot \cos \varphi = x_j \delta_{jk}$

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

Из выражений (2, 3) следует, что вектора, 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 $M_r \Rightarrow \{Y_1, Y_2, Y_4, Y_8, Y_{16}, \dots, Y_{2^n}\}$. 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 $Y_3 = Y_1 * Y_2$. Каждые последующие производные функции Уолша образуются согласно алгоритму:

$$\begin{aligned} Y_5 &= Y_1 * Y_4; \\ Y_6 &= Y_2 * Y_4; \\ Y_7 &= Y_1 * Y_2 * Y_4; \\ Y_9 &= Y_1 * Y_8; \dots; \\ Y_{15} &= Y_1 * Y_2 * Y_4 * Y_8; \end{aligned} \quad (5)$$



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 $Y_k \rightarrow W_k$.

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 последовательно 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 восьмизначного Windows-кода, отображающими первый символ естественного алфавита, затем из оставшихся ортогональных сигналов восемь закрепляются за разрядами второго символа кодируемого текста

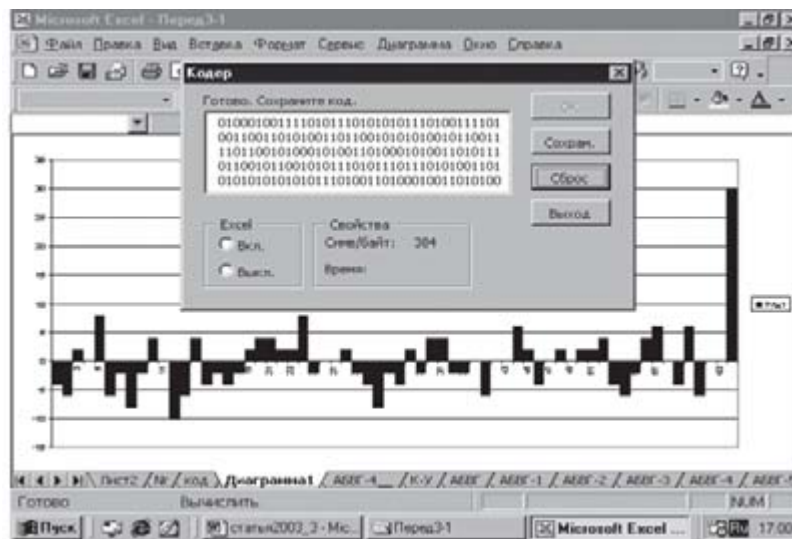


Рис. 3. Отображение слова «Криптон» сложным составным многоуровневым сигналом, состоящим из 56 ортогональных сигналов «Уолша»

и т. д. В результате такого преобразования все семь символов кодируемого текста отображаются на множестве ортогональных функций Уолша

$$\forall x_i \in X \rightarrow \{a_w\} | 8 \rightarrow \{y_i \in Y\} | 64 \quad (8)$$

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 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 [3, 4, 5].

На диаграмме рис.3 отображен сложный составной многоуровневый суммарный сигнал слова «Криптон», состоящий из 56 ортогональных сигналов Уолша ($Y_1 \dots Y_{56}$).

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 ме-

жду 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. График установления соответствий между кодовыми комбинациями и квантованными уровнями сложного составного суммарного сигнала задается программным методом или устанавливается самим пользователем.

Список используемой литературы

1. Качмаж С., Штейнгауз Г. Теория ортогональных рядов. М., Наука, 1958.
- а. Котельников В.А. Теория потенциальной помехоустойчивости. М., Радио и Связь, 1956.
- б. Макаров В.Ф. Теоретические основы передачи и защиты информации в системах теледиступа к вычислительным ресурсам. М., Академия управления МВД РФ, 1992.
- с. Макаров В.Ф., Нечаев Д.Ю. Методы защиты информационной инфраструктуры экономических систем. М., РГТЭУ, 2011.
2. Макаров В.Ф. Передача информации в компьютерных технологиях на основе ортогональных сигналов. Информационные системы и технологии, №2, 2014 г., Московский государственный инженерно-физический институт. 54-59 с.
3. Макаров В.Ф., Нечаев Д.Ю. Устранение избыточности в системах ортогонального кодирования. «Безопасность информационных технологий», №2, 2014 г., Московский государственный инженерно-физический институт. 54-59 с.
4. Макаров В.Ф. и др. Устройство для приема телевизионных сигналов. Патент на изобретение N2144741. Зарегистрирован в Государственном реестре изобретений РФ 20.01.2000.
5. Сюзев В.В. Основы теории цифровой обработки сигналов. М., РТСОфт, 2014.
6. Хармут Х. Теория секвентного анализа. Основы и применения. Пер. с англ., М., МИР, 1980.