

АНСАМБЛЕВЫЕ И КОРРЕЛЯЦИОННЫЕ СВОЙСТВА КРИПТОГРАФИЧЕСКИХ СИГНАЛОВ ДЛЯ ПРИЛОЖЕНИЙ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ

Введение

Кодовая адресация абонентов (множественный доступ с кодовым разделением абонентов) в многопользовательских телекоммуникационных системах (ТКС) предполагает, что каждый из абонентов передает и получает свои индивидуальные данные посредством использования некоторой специфической для пользователя дискретной последовательности (сигнатуры). При кодовом разделении имеют место взаимные помехи, которые являются следствием одновременной работы абонентов в общей полосе частот. Для обеспечения максимально возможной совместимости абонентов должны быть выполнены требования к свойствам сигнатур. Другими словами, при кодовом разделении можно так выбрать параметры сигналов, что уровень взаимных помех будет сколь угодно малым, т. е. будет обеспечена заданная помехоустойчивость. Существенная роль для обеспечения требуемой помехоустойчивости принадлежит корреляционным свойствам сигналов.

В широкополосных ТКС данные пользователя тем или иным способом модулируют сигнатуры или дискретные последовательности пользователя, образуя модулированный сигнал. Приемник должен выделить данные пользователя из принятого наблюдения. Однако наличие боковых пиков у функции неопределенности (ФН) сложных сигналов приводит к увеличению неоднозначности при совместном измерении дальности и скорости, к увеличению времени вхождения в синхронизм, ошибкам при решении задачи различения сигналов. Поэтому при выборе или синтезе сложных сигналов в процессе построения телекоммуникационной системы (ТКС) необходимо найти сигналы с малыми боковыми пиками ФН (сигналы с хорошими корреляционными свойствами). При этом необходимо определить влияние боковых пиков на характеристики обнаружения сигналов, измерения их параметров, различения сигналов, найти условия получения малых боковых пиков.

Основные результаты исследований

Среди всего многообразия сложных сигналов в широкополосных системах (частотно-модулированные, многочастотные, дискретные частотные, частотно-манипулированные и др.) важное место занимают периодические дискретные сигналы, получаемые манипуляцией начальных фаз радиоимпульсов по закону некоторой дискретной последовательности (ДП) периода L (фазоманипулированные сигналы).

Процесс выбора рациональных по тем или иным критериям структур сложных сигналов тождествен синтезу соответствующих манипулирующих ДП.

В теории сложных сигналов известен ряд интегральных равенств [1]. Пусть C – множество комплексных чисел, а C^N – множество векторов с комплексными компонентами. Элементы множества $w, x, y, z \in C^N$ – произвольные векторы, а w, x, y, z – соответствующие им дискретные последовательности. Четыре взаимно-корреляционные функции $R_{w,x}$, $R_{y,z}$, $R_{w,y}$, $R_{x,z}$ связаны соотношением

$$\sum_{l=0}^{N-1} R_{w,y}(l)[R_{x,z}(l+n)]^* = \sum_{l=0}^{N-1} R_{w,x}(l)[R_{y,z}(l+n)]^* . \quad (1)$$

Положив в (1) $z = y$, получим

$$\sum_{l=0}^{N-1} R_{w,y}(l)[R_{x,y}(l+n)]^* = \sum_{l=0}^{N-1} R_{w,x}(l)[R_y(l+n)]^* . \quad (2)$$

Положив в (2) $w = x$, получим

$$\sum_{l=0}^{N-1} R_{x,y}(l)[R_{x,y}(l+n)]^* = \sum_{l=0}^{N-1} R_x(l)[R_y(l+n)]^* . \quad (3)$$

Наконец, положив в (3) $n = 0$, получим

$$\sum_{l=0}^{N-1} |R_{x,y}(l)|^2 = \sum_{l=0}^{N-1} R_x(l)[R_y(l)]^* . \quad (4)$$

С помощью (1) – (4) получен ряд важных границ оценки корреляционных функций. Кроме того, использование этих соотношений приводит к полезным вычислительным алгоритмам и методам построения последовательностей. Так, тождество (1) означает, что, взаимно-корреляционная функция последовательностей $R_{w,y}$ и $R_{x,z}$ совпадает с взаимно-корреляционной функцией последовательностей $R_{w,x}$ и $R_{y,z}$. Если предположить, что последовательности w и x не коррелированы, тогда, согласно (1), последовательности $R_{w,y}$ и $R_{y,z}$ также не коррелированы. Причем отсутствие корреляции имеет место при произвольном выборе y и z . В частности, как видно из (2), последовательности y и z могут совпадать. Таким образом, при двух некоррелированных последовательностях могут быть построены две новые последовательности с такими же свойствами. Равенство (3) означает, что автокорреляционная функция последовательности $R_{x,y}$ совпадает взаимно-корреляционной функцией последовательностей R_x и R_y . Пусть последовательности x и y – последовательности периода L с двухуровневой автокорреляцией. Тогда последовательности $R_{x,y}$ и $R_{y,x}$ также имеют период L и обладают двухуровневыми автокорреляционными функциями. Кроме того, из (4) следует, что среднее значение квадрата модуля функции взаимной корреляции сигналов x и y равно среднему значению произведения их автокорреляционных функций. Фактически это означает, что сигналы, обладающие хорошими автокорреляционными свойствами, будут обладать и хорошими свойствами взаимно-корреляционных функций.

При выборе критерия выбора структур (систем) сложных сигналов, как правило, ориентируются на минимаксный критерий (критерий минимума взаимных помех). Такой критерий подразумевает построение ансамблей сигналов объема M , манипулированных ДП, как можно заметнее отличающихся друг от друга. Количественной мерой отличия ДП служат максимальные по ансамблю уровни бокового лепестка R_a периодической автокорреляционной функции (ПАКФ) и уровня R_b периодической взаимной корреляционной функции (ПВКФ), определяемые как

$$R_a = \max_l \|a_l\|^{-1} |R(m)|, m \neq 0 \bmod L, \quad (5)$$

$$R_b = \max_l \|a_l\|^{-1} \|a_s\|^{-1} |R_{em}(m)|, l \neq S; l, S = 0, 1, \dots, N-1, \quad (6)$$

где $R_{l,S}(m) = \sum_{i=1}^{L-1} a_{l,i+m} \cdot a_{s,i}^*$; $\|a_r\|$ – Евклидова норма кодового вектора $a_r = (a_{r,0}, a_{r,1} \dots a_{r,L-1})$

Наличие в L -мерном линейном пространстве не более L ортогональных векторов делает гипотетическим идеальный, с точки зрения минимаксного критерия, ансамбль ДП с нулевыми R_a и R_b и ограничивает потенциал снижения корреляционного выброса при фиксированных M и L .

Граница для максимальных значений корреляционных функций R_a , R_b в ансамблях M ДП длины L , составляет [2]

$$R_{\max} = \max\{R_a, R_b\} \geq L \left[\frac{M-1}{L \cdot M - 1} \right]^{1/2} \quad (7)$$

В ряде приложений систем связи (телекоммуникационных систем) (например, задачи измерения запаздывания и разрешения во времени) существенными являются периодические и аperiodические функции автокорреляции (ПАКФ). Применительно к указанным задачам, автокорреляционная функция сигнала должна иметь достаточно острый центральный пик и по возможности наиболее низкий уровень боковых лепестков. Известны границы максимальных значений боковых лепестков ПАКФ [2]:

$$R_a = \begin{cases} 0 & , \text{если } L \equiv 0(\text{mod } 4); \\ 1 & , \text{если } L \equiv 1(\text{mod } 4); \\ 2 & , \text{если } L \equiv 2(\text{mod } 4); \\ -1 & , \text{если } L \equiv 3(\text{mod } 4). \end{cases} \quad (8)$$

Приведенные границы устанавливают критерий синтеза множества ДП (сигнатур). Ансамбль из большого количества сигнатур может считаться подходящим, если значения функций авто- и взаимной корреляции близки к границам (7), (8) соответственно. Ансамбли, со значениями R_{\max} достигающие предела, предсказываемого границами (7) и (8), являются оптимальными по критерию корреляционного пика, и называются минимаксными. К числу таких ансамблей можно отнести криптографические ДП, метод синтеза которых приведен в [3].

Метод синтеза систем криптографических дискретных последовательностей включает следующие этапы:

1) Генерация массива псевдослучайных последовательностей символов заданного периода с использованием генератора ключей криптографического алгоритма, например AES;

2) Тестирование полученных последовательностей с применением критериев и показателей качества генераторов, определенных международными и ведомственными стандартами FIPS PUB 140-1 [4], FIPS PUB 140-2 [5], AIS 20 [6] и AIS 31 [7];

3) Формирование дискретных последовательностей символов фиксированного периода (например: 31, 53, 127, 255, 1023, 2047, ...);

4) Отбор ДП, значения боковых лепестков ПАКФ которых близких к границе (7), (8);

5) Получение матрицы состояний взаимно-корреляционных функций всех возможных пар последовательностей, прошедших отбор по результатам предыдущего шага;

4) Формирование границ предельных значений («плотной упаковки») для различных корреляционных функций (функции авто- и взаимной корреляции в периодическом и аperiodическом режимах);

5) Обработка матрицы, заключающаяся в том, что осуществляется отбор последовательностей, удовлетворяющих границам «плотной упаковки» для соответствующих корреляционных функций.

В качестве иллюстраций на рис. 1 – 3 приведены различные функции корреляции для синтезированных в соответствии с описанными выше правилами криптографических ДП.

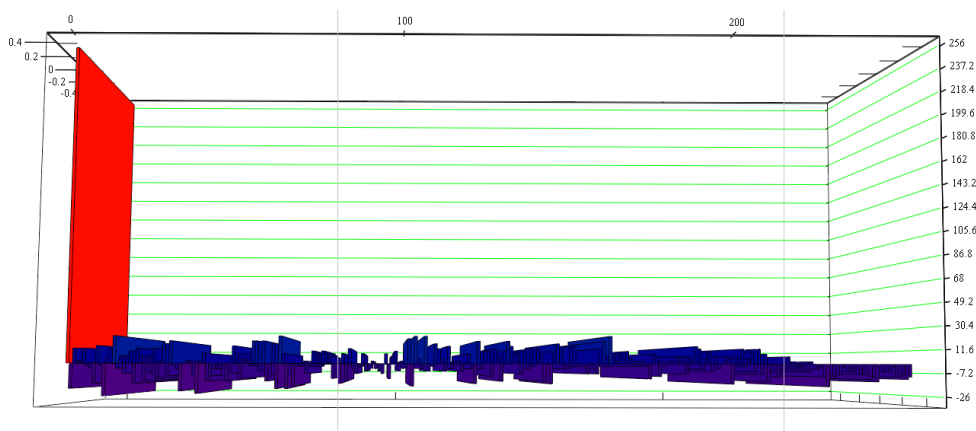


Рис. 1. Вид АФАК для КП периода $L = 256$

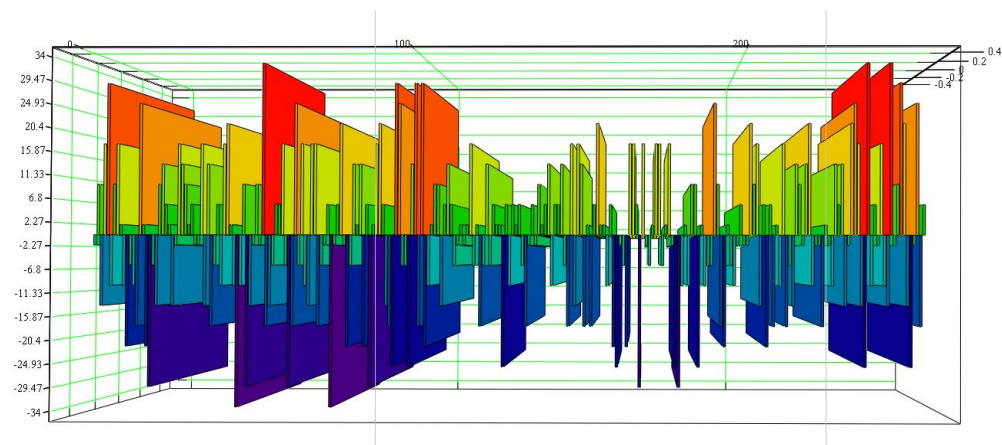


Рис. 2. Вид ПФВК для КП периода $L = 256$

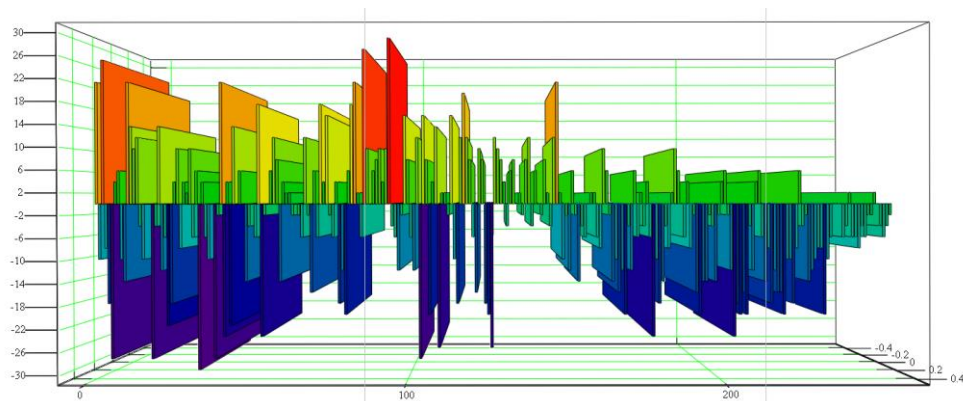


Рис. 3. Вид АФВК для КП периода $L = 256$

При работе ТЛКС в условиях действия мощных взаимных помех отношение сигнал/помеха на выходе согласованного фильтра зависит от значений боковых пиков функции взаимной корреляции. Из этого следует правило выбора сигналов, образующих систему:

необходимо выбирать сигналы, у которых максимальные пики функции взаимной корреляции минимальны.

В табл. 1 приведены примеры расчета статистических характеристик различных корреляционных функций для широко используемых в системах связи дискретных сигналов и, в том числе, характеристики криптографических ДП. Расчеты проводились для различных значений периода ДП. В качестве статистических характеристик корреляционных функций были использованы:

- значения наибольших боковых выбросов u_{\max} ;
- величина математического ожидания модуля выбросов $m_{|u|}$;
- значение среднеквадратического отклонения модуля выбросов $D_{|u|}^{1/2}$ и значения

выбросов $D_u^{1/2}$.

Таблица 1

Статистические характеристики
корреляционных функций дискретных сигналов

Тип сигналов	Характеристики	$\frac{u_{\max}}{\sqrt{L}}$	$\frac{m_{ u }}{\sqrt{L}}$	$\frac{D_{ u }^{1/2}}{\sqrt{L}}$	$\frac{D_{(u)}^{1/2}}{\sqrt{L}}$
ХДС	АФАК	1,0	0,5	0,4	0,5
	ПФАК	0,2	0,2	0,1	0,2
	МИФАК	2,6	0,6	0,5	0,8
	АФВК	2,1	1,0	0,8	1,0
	ПФВК	2,3	1,0	0,8	1,2
	СФВК	2,3	0,9	0,7	1,1
ЛРПМ	АФАК	0,7...1,25	0,32	0,26	0,41
	ПФАК	$1/\sqrt{L}$	$1/\sqrt{L}$	0	0
	МИФАК	1,3...2,3	0,66	0,49	0,82
	АФВК	1,4...5,0	0,54	0,48	0,73
	ПФВК	1,9...6,0	0,8	0,62	1,0
	СФВК	2,0...5,1	0,83	0,62	1
Криптографические последовательности	АФАК	1,6	0,5	1	1,1
	ПФАК	1,7	0,6	0,4	0,7
	АФВК	1,3	0,5	0,4	0,6
	ПФВК	1,8	0,7	0,5	0,8

Анализ данных, приведенных в табл. 1, свидетельствует о том, что значения максимальных боковых выбросов КП, а также статистические характеристики данного класса сигналов не уступают соответствующим характеристикам М-последовательностей.

Среди фазоманипулированных сигналов М-последовательности занимают особое место, что обусловлено рядом замечательных свойств данного класса сигналов: простота устройств формирования, хорошие корреляционные и «шумоподобные» свойства, существование пар последовательностей, которые приводят к сигналам с улучшенными взаимно-корреляционными свойствами и др. При этом необходимо отметить, что М-последовательности порождаются двоичным полиномом степени n

$$h(x) = h_0x^n + h_1x^{n-1} + \dots + h_{n-1}x + h_n, \quad (9)$$

где $h_0 = h_n = 1$, а другие h_i принимают значения 0 или 1.

Такие последовательности получают с помощью n -каскадного сдвигового регистра с линейной цепью обратной связи, к которым подключены отводы от каскадов с номерами,

для которых $h_i = 1$. Правило построения М-последовательностей обусловило одно из свойств данного класса сигналов (и других классов сигналов, в основе построения которых лежат линейные законы построения) – низкая структурная скрытность сигнала. Известно, что для определения правила построения М-последовательности (двоичного полинома степени n) необходимо владеть сегментом из $2n$ подряд следующих символов. Например: если степень полинома $n = 256$ (период такой последовательности $2^{256} - 1 = 1,16 \cdot 10^{77}$), то для определения правила построения последовательности, полученной с использованием данного полинома, необходимо знать сегмент из 512 двоичных символов. Кроме того, объем системы данного класса сигналов ограничен и составляет

$$M = \varphi(L/n),$$

где $\varphi(L)$ – функция Эйлера.

Вместе с тем, для ряда приложений телекоммуникационных систем требуются сигналы, обладающие высокой структурной скрытностью, необходимыми корреляционными свойствами и значительным объемом системы сигналов.

В табл. 2 приведены данные, характеризующие корреляционные свойства КП различного периода, в частности: граничные значения боковых пиков автокорреляционных функций, достигаемых в классе М-последовательностей и число сигналов, удовлетворяющих данной границе в классе КП для различных функций корреляции; наименьшие значения боковых пиков различных функций корреляции и их количество; объем системы сигналов (в том числе, количество пар КП, удовлетворяющих граничным значениям для соответствующего периода последовательности) и др.

Таблица 2

Корреляционные свойства криптографических дискретных последовательностей

№ п/п	Размерность сегмента КП	Граничные значения функции неопределенности	ПФАК			АФАК	ПФВК			АФВК
			Число КП удовлетворяющих границе	Наименьшее значение $R_{\text{бmax}}$	Количество КП с наименьшим $R_{\text{бmax}}$	Количество КП, удовлетворяющих границе	Общее количество пар	Количество пар, удовлетворяющих границе	Наименьшее значение $R_{\text{бmax}}$	Количество пар, удовлетворяющих границе
1	31	9	7 743	5	155	3 622	29 977 024	1 465 137	5	14 537 423
2	63	17	10 868	9	14	7 166	59 056 712	12 214 869	11	54 822 445
3	127	23	3482	17	51	1302	6 062 162	47 053	19	1 619 780
4	511	59	3819	45	6	1951	7 292 380	122 835	51	3 466 713
5	1 023	100	8 513	77	9	6 194	36 235 584	5 293 538	79	35 083 491

В табл. 3 приведены (с учетом данных табл.2) данные, характеризующие ансамблевые свойства криптографических ДП в сравнении с М-последовательностями и последовательностями с трехуровневой ПФВК.

Анализ данных в табл. 2, 3 показывает, что КП обладают существенно лучшими ансамблевыми свойствами по сравнению с М-последовательностями и последовательностями с трехуровневой ПФВК.

Таблица 3

Ансамблевые свойства различных систем сложных сигналов

Класс сигналов	Период последовательности	Значение границы «плотной упаковки»	Число пар последовательностей, удовлетворяющих границе
Линейные:			
М-последовательности	31	9	3
Последовательности с трехуровневой ПФВК	31	9	495
Нелинейные криптографические последовательности	31	9	1465137
Линейные:			
М-последовательности	127	27	36
Последовательности с трехуровневой ПФВК	127	17	11610
Нелинейные криптографические последовательности	127	23	47 053
Линейные:			
М-последовательности	255	36	28
Последовательности с трехуровневой ПФВК	–	–	–
Нелинейные криптографические последовательности	255	36	17599
Линейные:			
М-последовательности	511	63	276
Последовательности с трехуровневой ПФВК	511	33	147500
Нелинейные криптографические последовательности	511	63	2666671
Линейные:			
М-последовательности	1023	100	435
Последовательности с трехуровневой ПФВК	1023	65	338000
Нелинейные криптографические последовательности	1023	100	5293538

Выводы

Синтез систем дискретных последовательностей, обеспечивающих требуемые значения помехоустойчивости, информационной скрытности на уровне источника сложных сигналов, является перспективным направлением исследований. В работе представлены результаты исследований свойств нового класса дискретных последовательностей. Показано, что сигналы, построенные путем манипуляции такими дискретными последовательностями информационных битов, обладают, с одной стороны, структурными свойствами, аналогичными свойствам случайным последовательностям, а с другой – корреляционными свойствами, близкими к свойствам линейных классов сигналов, в частности М-последовательностей. При этом ансамблевые свойства нового класса сигналов существенно лучше ансамблевых свойств М-последовательностей.

Список литературы: 1. *Сарватте Д., Персли М.* Взаимно-корреляционные свойства псевдослучайных и родственных последовательностей // ТИИЭР. – 1980. – Т.68, № 5. – С. 59-90. 2. *Свердлик М. Б.* Оптимальные дискретные сигналы. / Свердлик М. Б. – М. : Радио и связь, 1975. – 200 с. 3. *Замула А.А.* Перспективы применения нелинейных дискретных сигналов в современных телекоммуникационных системах и сетях / Замула А.А., Семенко Е.А // Системы обработки информации:– X. : ХУПС, 2015. – Вип. 5 (130). – С. 129 – 134. 4. Federal Information Processing Standards Publication (FIPS PUB) 140-1. Security requirements for cryptographic modules. NIST, 1994. 5. Federal Information Processing Standards Publication (FIPS PUB) 140-2. Security requirements for cryptographic modules. NIST, 1999. 15. Application Notes and Interpretation of the Scheme (AIS) 31. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 2001. 6. Application Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 1999. 7. Federal Information Processing Standards Publication (FIPS PUB) 140-1. Security requirements for cryptographic modules. NIST, 1994.

*Харьковский национальный университет
имени В.Н. Каразина*

Поступила в редколлегию 15.04.2015