УДК 004.9

А.А. Замула, В.Л. Морозов, Д.А. Семченко

Харьковский национальный университет имени В.Н. Каразина, Харьков

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ СИНТЕЗА ПРОИЗВОДНЫХ СИСТЕМ СИГНАЛОВ ДЛЯ ПРИЛОЖЕНИЙ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ

Сформулированы требования к выбору систем сложных сигналов - переносчиков данных для применения в информационно-коммуникационных системах (ИКС), для которых предъявляются повышенные требования по обеспечению помехозащищенности, помехоустойчивости, скрытности функционирования и информационной безопасности информации. Представлены концептуальные основы синтеза нового класса сложных сигналов - криптографических сигналов (КС). Обосновывается целесообразность применения КС в защищенных ТКС, в том числе, при формировании производных систем сигналов, с целью улучшения показателей помехозащищенности, помехоустойчивости, скрытности функционирования и информационной безопасности данных в защищенных ИКС.

Ключевые слова: *информационная безопасность, скрытность, помехозащищенность, система сигналов, производные системы сигналов, широкополосные системы.*

Введение

В условиях интенсивного противодействия сторон, интересы и конкуренция которых могут проявляться в различных сферах, в том числе, как показали последние события, в сфере ведения информационных и гибридных войн, особое значение приобретает наличие и применение защищенных информационно-коммуникационных систем (ИКС). При этом под защищенностью систем необходимо понимать, в широком смысле, прежде всего, их способность обеспечивать необходимые показатели по помехозащищенности, имитостойкости, информационной, энергетической и структурной скрытности функционирования системы.

К ИКС предъявляются все более жесткие требования по обеспечению эффективности их функционирования в условиях сложных внешних воздействий: естественных и преднамеренных помех, помех от других радиотехнических систем, функционирующих на близких частотах или в общем участке диапазона частот. Большое значение при решении задач обеспечения требуемой помехозащищенности и информационной безопасности имеют исследования, связанные с использованием новых видов сигналов, получивших название сложных, широкополосных, многомерных и шумоподобных.

Задача построения защищенной ИКС – создать систему, устойчивую к воздействию множества различных, актуальных для данной системы, воздействий (помех). Объективной проблемой является то, что в процессе информационного обмена соответствие: бит сообщение-сигнал является фиксированным, а в качестве переносчиков информации, используются сигналы, построенные с применением линейных правил. Вышеуказанное позволяет нарушителю, на основе определения параметров используемых в системе сигналов, осуществить постановку помех с минимальными для себя энергетическими затратами. Существуют угрозы информационной безопасности, а именно, возможность: несанкционированного доступа к информационным активам, нарушение целостности, конфиденциальности, доступности данных со стороны злоумышленников.

Основными путями решения указанной проблемы является повышение помехозащищенности и информационной безопасности ИКС на основе усовершенствования методологических основ построения ИКС путем создания новых моделей, методов и технологий управления телекоммуникационными сетями, информационной безопасностью, услугами и качеством обслуживания, разработки методов информационного обмена, методов синтеза новых классов нелинейных дискретных сложных сигналов с необходимыми ансамблевыми, корреляционными и структурными свойствам.

В статье предлагается метод синтеза дискретных последовательностей с заданными взаимнокорреляционными, структурными и ансамблевыми свойствами для применения в телекоммуникационных системах, в которых предъявляются повышенные требования к обеспечению скрытности, помехозащищенности, помехоустойчивости, информационной безопасности функционирования системы.

Различение или кодовое разделение абонентов многопользовательской ИКС основано на том, что каждому абоненту выделяется алфавит сигналов (кодовых последовательностей), с помощью которого абонент передает информацию. Наиболее часто используемым критерием различимости является минимум эвклидового расстояния [1]. Критерий состоит в том, что два сигнала являются легко различимыми тогда и только тогда, когда среднеквадратичное расстояние между ними велико. Необходимость совместного рассмотрения сигналов Y(t) и X(t) возникает при использовании манипуляции, например, в тех случаях,

когда сигнал X(t) модулируется двоичной последовательностью или когда им самим модулируется некоторая несущая. Таким образом, в качестве меры различимости сигналов используют величину:

$$T^{-1}\int_0^T [Y(t) \pm X(t)]^2 = \\ = -T^{-1}\left\{\int_0^T [Y^2(t) + X^2(t)]dt \pm 2\int_0^T X(t)Y(t)dt\right\}, \quad (1)$$

где T - период сигналов X(t) и Y(t).

Первый интеграл в правой части (1) есть сумма энергий сигналов X(t) и Y(t), $0 \le t \le T$. Следовательно, при фиксированных энергиях сигнал X(t) сильно отличается как от сигнала X(t), так и от сигнала –X(t) только в том случае, когда мал параметр

$$R = \int_0^T X(t)Y(t)dt . \quad (2)$$

.Параметр R при решении задач поиска, обнаружения, оценки параметров, (в этом случае используется согласованная фильтрация или корреляционный прием), представляет собой отклик согласованного с сигналом Y(t) фильтра на входной сигнал X(t). Например, если в многопользовательской ИКС с кодовым разделением сигналы X(t) и Y(t) выделены двум различным станциям (абонентам), то параметр R является мерой уровня взаимных помех, создаваемых каждым из сигналов приему другого.

В ИКС в качестве физического переносчика информации нашли применение различные системы (множества линейных рекуррентных последовательностей, Касами, Голда, Камалетдинова и др.), обладающие сравнительно небольшими значениями боковых лепестков авто и взаимно - корреляционных функций [2]. Однако указанные сигналы обладают низкой структурной скрытностью, ограниченными ансамблевыми свойствами, а также существуют только для ограниченного числа значений периода сигнала. В случае усечения (увеличения) периода таких сигналов их корреляционные свойства ухудшаются. Поэтому актуальной является задача разработки теории и практики синтеза и анализа систем дискретных сигналов с требуемыми корреляционными, структурными, ансамблевыми свойствами.

Исследования показали [3], что требуемые (в тех или иных условиях) показатели эффективности функционирования системы могут быть реализованы, в том числе, посредством применения широкополосных радиосистем, для которых расширение спектра осуществляется с применением нелинейных дискретных последовательностей.

В некоторых ИКС число одновременно используемых сигналов может превышать несколько сотен. Известны большие множества периодических последовательностей (множества Касами, Голда), обладающие корреляционными функциями со сравнительно небольшими значениями боковых лепестков взаимно-корреляционных функций. Для генерации таких последовательностей применяются сдвиговые регистры с линейной обратной связью. Правила построения указанных классов последовательностей указывают на низкую структурную скрытность формируемых последовательностей, а, следовательно, и сигналов, обеспечивающих передачу информации в телекоммуникационных системах. Здесь под структурной скрытностью понимается сложность определения злоумышленником правила (закона) построения дискретной последовательности, используемой для манипуляции информационных битов.

Необходимость применения защищенных радиоканалов вынуждает исследователей по-новому посмотреть как на режимы функционирования защищенных радиоканалов, так и на аспекты формирования и применения сложных сигналов. Поэтому, на наш взгляд, сегодня необходимы новые подходы и новые взгляды на процессы применения и функции сложных сигналов в целях построения защищенных ИКС. Основополагающим здесь, на наш взгляд, является новое понимание методов обеспечения информационной скрытности и имитостойкости, то есть функций, которые в традиционных системах реализуются с применением систем и средств криптографической защиты информации. Продуктивным шагом, с точки зрения нового направления использования систем сложных сигналов, является синтез так называемых систем криптографических сигналов. Синтез таких сигналов основывается на применении ключевых данных.

Для защищенных радиоканалов рассматриваемые системы сигналов определяются приложениями, в которых они применяются. В частности, это могут быть как отдельные сигналы или пары сигналов, так и большие множества дискретных сигналов с необходимыми, но объективно ограниченными значениями «плотной упаковки», взаимно-корреляционными и ансамблевыми свойствами.

Под криптографическим дискретным сигналом предлагается понимать последовательность символов произвольного алфавита и произвольного периода, единственным правилом построения которого есть случайность или псевдослучайность. Такой дискретный сигнал обладает необходимыми, но ограниченными значениями «плотной упаковки», корреляционными и ансамблевыми свойствами. При таком подходе структурная скрытность сигнала обеспечивается посредством случайности или псевдо случайности.

В работе [4] сформулирована и решена задача синтеза нелинейных криптографических дискретных сигналов (КС), обеспечивающих требуемые значения помехозащищенности, информационной и структурной скрытности функционирования телекоммуникационной системы. В общем случае задача синтеза оптимальных бинарных криптографических сигналов заданного периода, формулируется следующим образом. Необходимо найти множество дискретных двоичных последовательностей – криптографических последовательностей (КП) с заданным числом символов, обладающих допустимым

уровнем максимальных боковых лепестков периодической функции автокорреляции (ПФАК). Далее, решение задачи синтеза сводится к предварительному отбору некоторого ограниченного множества дискретных последовательностей, которое кажется многообещающим в плане обеспечения необходимых взаимно - корреляционных свойств.

Необходимо отметить, что в процессе исследований была высказана гипотеза о возможности применения криптографического алгоритма в целях синтеза системы сигналов. Для этих целей был обоснован выбор Национального криптографического стандарта блочного симметричного преобразования ДСТУ 7624:2014, определяющий шифр „Калина" [5].

В табл. 1 приведены результаты синтеза КС для некоторых значений периода последовательностей. Анализ данных табл. 1 показывает, что для периода последовательности, например, 63 число пар КС, соответствующие установленному предельному значению 17 составляет более $12 \cdot 10^6$ (12214869). Для последовательностей с трехуровневой функцией взаимной корреляции (ФВК), число пар, соответствующие данной «границы» составляет лишь 975 пар. Таким образом, ансамбль нелинейных КС более чем в 10^5 раз превышает ансамбль указанных линейных сигналов. Превышение объема криптографических сигналов над ансамблем, составленного из М-последовательностей составляет более 10^7 раз.

Синтез производных систем сигналов на основе криптографических дискретных последовательностей символов

Среди систем фазоманипулированных сигналов многие образованы на базе систем Уолша [2]. Известно, что авто - и взаимно корреляционные функции последовательностей Уолша имеют большие боковые пики. Для улучшения корреляционных свойств сигналов формируют производные системы сигналов (ПСС) посредством перемножения последовательностей Уолша (исходных последовательностей) на сигнал, который обладает определенными свойствами (производящий сигнал), в частности, имеют малые боковые пики автокорреляционной функции.

Таблица 1

Ансамблевые свойства криптографических сигналов

Период КС	ПУ	ПФАК	АФАК	ПФВК		АФВК
		$N_{ПУ}$	$N_{ПУ}$	N	$N_{ПУ}$	$N_{ПУ}$
31	9	7 743	3 622	29 977 024	1 465 137	14 537 423
63	17	10 868	7 166	59 056 712	12 214 869	54 822 445
127	23	3482	1302	6 062 162	47 053	1 619 780
511	59	3819	1951	7 292 380	122 835	3 466 713
1 023	100	8 513	6 194	36 235 584	5 293 538	35 083 491

В таблице обозначено: N – общее число пар сигналов; $N_{ПУ}$ – число КС, удовлетворяющих границе «плотной упаковки»; ПУ – граничные значения («Плотная упаковка»).

Авторами была сформулирована гипотеза о возможности использования в качестве производящих – нелинейных криптографических последовательностей (КП), теоретические основы синтеза которых приведены в [4]. Метод синтеза производных систем сигналов на основе использования КС включает следующие этапы.

1. Осуществляется отбор М криптографических последовательностей (КП) фиксированного периода N, обладающих минимальными значениями максимальных боковых лепестков ($R_{max.}$) ПФАК.

2. Формируется набор кодов Уолша (матрица N·N), в которой каждая строка соответствует отдельному коду.

3. Выполняют перемножения последовательностей (каждой из строк кода Уолша - исходных последовательностей) на криптографический сигнал, образуя N ПСС.

4. Осуществляют исследование корреляционных свойств образованных ПСС (в частности, ПФАК, АФАК). Для исследования функций взаимной корреляции, образуют матрицу размерностью N·N. Число таких матриц: L·N.

В табл. 2 приведены КП (M = 14), отобранные из множества последовательностей, по критерию минимума значений максимальных боковых лепестков ПФАК ($R_{max} < 10$), на основе матрицы Адамара (N = 64). Здесь же приведены расчеты статистических характеристик корреляционных функций (ПФАК) отобранных КС (рис. 1).

В табл. 3 приведены результаты исследований статистических характеристик корреляционных функций различных классов сигналов, в том числе, ПСС при использовании в качестве производящих - криптографических сигналов. Расчеты проводились для значений периодов последовательностей (от 30 до 2052).

Анализ данных табл. 3 показывает, что статистические характеристики ПСС близки к соответствующим характеристикам, указанным в таблице, линейных и нелинейных классов сигналов. При этом значения максимальных боковых пиков функций взаимной корреляции ПСС меньше, чем у широко используемых в современных телекоммуникационных системах линейных М последовательностей.

Результаты исследования ПФВК ПСС на основе КП показывают, что число пар сигналов для периода последовательностей 64 символов, для которых значения R_{max} не превышают 17 (это, так называемая, граница «плотной упаковки», достигаемая в классе лучших, с точки зрения ВКФ, последовательностей с трехуровневой ПФВК), составляет 604 пары (около 30% из общего числа возможных сочетаний пар сиг-

налов). Число пар сигналов, для которых значения R_{max} не превышают 20 – 1577, что составляет 77% от общего числа пар сигналов. При границе $R_{max} < 25$ - максимальное количество отобранных пар сигналов составляет 1984 (96,8 %). Такие значения R_{max} имеют место для последовательностей, получивших наибольшее распространение в современных телекоммуникационных системах - М-последовательности.

Таблица 2

КС, имеющие минимальные значения боковых лепестков ПФАК

1	1 1 1 0 0 0 1 1 1 1 1 0 1 0 0 0 0 1 1 1 1 1 0 1 1 1 0 0 1 1 0 0 1 1 0 0 0 1 0 1 0 0 0 1 1 0 1 0 1 1 0 1 0 0 1 0 0 1 1 0 0 1 0 1
2	1 0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1
3	0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1
4	0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1
5	0 0 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0
6	0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 0 0
7	0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 0 0 1 0 1 1 0
8	0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 0 0 1 0 1 1 0 1
9	0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 0 0 1 0 1 1 0 1 0
10	0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 0 0 1 0 1 1 0 1 0 0
11	0 0 0 0 0 0 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0 1 1 0 1 1 0 1 1 1 0 0 0 1 1 0 1 0 0 0 0 1 0 1 1 1 1 0 0 1 0 1
12	0 0 0 0 0 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0 1 1 0 1 1 0 1 1 1 0 0 0 1 1 0 1 0 0 0 0 1 0 1 1 1 1 0 0 1 0 1 0
13	0 0 0 0 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0 1 1 0 1 1 0 1 1 1 0 0 0 1 1 0 1 0 0 0 0 1 0 1 1 1 1 0 0 1 0 1 0 0
14	0 1 0 0 0 1 1 1 1 0 0 0 1 1 0 0 0 0 0 1 0 0 1 1 0 0 1 0 0 0 0 0 0 0 0 1 1 0 1 1 1 1 1 0 1 1 1 0 0 1 0 1 0 1 1 0 0 0 0 1 0 1 1 0

1)64 0 -8 -4 -4 0 -8 0 0 4 0 4 4 -8 -4 8 -4 -4 0 4 4 -4 4 -4 0 8 4 4 -4 -8 -4 0 -8 0 -4 -8 -4 4 4 8 0 -4 4 -4 4 4 0 -4 -4 8 -4 -8 4 4 0 4 0 0 -8 0 -4 -4 -8
0 PFAKmin: -4 PFAKmax: -8 MO: -0.09375 |MO|: 0.46875 DISP: 0.5763694553724894 |DISP|: 0.3384787011890674
2)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 8 4 4 8 -8 8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4
PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576
3)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 8 4 4 8 -8 8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4
PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576
4)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 8 4 4 8 -8 8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4
PFAKmin: 4 PFAKmax: -8MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576
5)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 8 4 4 8 -8 8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4
PFAKmin: 4 PFAKmax: -8MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576
6)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 8 4 4 8 -8 8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4
PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576
7)64 4 -8 4 4 0 0 4 -4 4 0 -8 4 0 4 0 4 0 -8 0 0 8 0 0 -8 -4 -4 4 8 4 4 4 -4 4 4 4 8 4 -4 -4 -8 0 0 8 0 0 -8 0 4 0 4 0 4 -8 0 4 -4 4 0 0 4 4 -8 4
PFAKmin: 4 PFAKmax: -8 MO: 0.0703125 |MO|: 0.4296875 DISP: 0.5553298776598447 |DISP|: 0.350712702793093
8)64 0 -8 4 4 0 -4 4 -8 8 4 -8 4 0 8 0 0 4 -8 0 -4 4 0 0 -8 -4 0 0 0 4 4 0 0 0 0 4 4 0 0 -4 -8 0 0 4 -4 0 -8 4 0 0 8 0 4 -8 4 8 -8 4 -4 0 4 4 -8 0
PFAKmin: 4 PFAKmax: -8 MO: 0.0 |MO|: 0.40625 DISP: 0.5634361794742422 |DISP|: 0.3836429502240921
9)64 0 -8 4 4 0 -4 4 -8 8 4 -8 4 0 8 0 0 4 -8 0 -4 4 0 0 -8 -4 0 0 0 4 4 0 0 0 0 0 4 4 0 0 -4 -8 0 0 4 -4 0 -8 4 0 0 8 0 4 -8 4 8 -8 4 -4 0 4 4 -8 0
PFAKmin: 4 PFAKmax: -8 MO: 0.0 |MO|: 0.40625 DISP: 0.5634361794742422 |DISP|: 0.3836429502240921
10)64 0 -8 4 4 0 -4 4 -8 8 4 -8 4 0 8 0 0 4 -8 0 -4 4 0 0 -8 -4 0 0 0 4 4 0 0 0 0 0 0 4 4 0 0 -4 -8 0 0 4 -4 0 -8 4 0 0 8 0 4 -8 4 8 -8 4 -4 0 4 4 -8 0
PFAKmin: 4 PFAKmax: -8 MO: 0.0 |MO|: 0.40625 DISP: 0.5634361794742422 |DISP|: 0.3836429502240921
11)64 8 4 0 -8 -8 -4 4 8 8 4 0 0 -4 -8 4 8 8 0 8 4 0 0 -4 -4 -8 -4 0 0 4 -4 4 -4 -4 4 4 0 0 -4 -8 -4 -4 0 0 4 8 0 8 8 4 -8 -4 0 0 4 8 8 4 -4 -8 -8 0 4 8
PFAKmin: 4 PFAKmax: 8 MO: 0.0703125 |MO|: 0.5234375 DISP: 0.6476900319675074 |DISP|: 0.3767205345969094
12)64 8 4 0 -8 -8 -4 4 8 8 4 0 0 -4 -8 4 8 8 0 8 4 0 0 -4 -4 -8 -4 0 0 4 -4 4 -4 -4 4 4 0 0 -4 -8 -4 -4 0 0 4 8 0 8 8 4 -8 -4 0 0 4 8 8 4 -4 -8 -8 0 4 8
PFAKmin: 4 PFAKmax: 8 MO: 0.0703125 |MO|: 0.5234375 DISP: 0.6476900319675074 |DISP|: 0.3767205345969094
13)64 8 4 0 -8 -8 -4 4 8 8 4 0 0 -4 -8 4 8 8 0 8 4 0 0 -4 -4 -8 -4 0 0 4 -4 4 -4 -4 4 4 0 0 -4 -8 -4 -4 0 0 4 8 0 8 8 4 -8 -4 0 0 4 8 8 4 -4 -8 -8 0 4 8
PFAKmin: 4 PFAKmax: 8 MO: 0.0703125 |MO|: 0.5234375 DISP: 0.6476900319675074 |DISP|: 0.3767205345969094
14)64 8 -4 4 4 0 0 4 -4 -4 4 -4 -8 0 -4 0 8 0 8 -4 -8 -4 -8 8 -8 0 0 4 0 -4 4 4 8 4 4 -4 0 4 0 0 -8 8 -8 -4 -8 -4 8 0 8 0 -4 0 -8 -4 4 -4 -4 4 0 0 4 4 -4
8 PFAKmin: -4 PFAKmax: 8 MO: 0.0 |MO|: 0.5 DISP: 0.6236095697723273 |DISP|: 0.3618734420321171

Рис. 1. Расчет статистических характеристик корреляционных функций (ПФАК) КС

Таблица 3

Статистические характеристики корреляционных функций различных классов сигналов

Тип сигналов	Характеристики	$R_{макс}/\sqrt{N}$	$m_{\|R\|}/\sqrt{N}$	$D^{1/2}_{\|R\|}/\sqrt{N}$	$D^{1/2}_{(R)}/\sqrt{N}$
Нелинейные характеристические последовательности	АФАК	1,6 - 2,4	0,3 - 3,4	1,4 - 7,7	1,9 - 10,8
	ПФАК	0,02 - 0,5	0,02 - 0,3	0,03 - 0,3	0,06 - 05
	АФВК	1,3 - 3,3	0,5 - 0,7	2,4 - 18,2	3,6 - 27
	ПФВК	0,8 - 3,3	0,7 - 0,8	5,8 - 45,3	5,9 - 45,3
ПСС	АФАК	0,8 - 2,4	0,4 - 0,5	0,9 - 1	1 - 1,1
	ПФАК	0,7 - 2,5	0,2 - 0,7	0,2 - 0,5	0,3 - 0,9
	АФВК	1 - 2,5	0,2 - 0,7	0,2 - 0,5	0,3 - 0,7
	ПФВК	1,4 - 2,8	0,2 - 0,7	0,4 - 0,5	0,6 - 0,9
Нелинейные криптографические последовательности	АФАК	0,7 - 2,5	0,4 - 0,5	0,9 - 1	0,9 - 1,2
	ПФАК	0,9 - 2,5	0,3 - 0,7	0,2 - 0,5	0,3 - 0,9
	АФВК	1,2 - 2,7	0,4 - 0,7	0,3 - 0,5	0,5 - 0,7
	ПФВК	1,5 - 2,8	0,5 - 0,7	0,3 - 0,5	0,8 - 0,9
Линейные М – последовательности	АФАК	0,7 - 1,25	0,32	0,26	0,41
	ПФАК	$1/\sqrt{N}$	$\sqrt{N}$	0	0
	АФВК	1,4 – 5,0	0,54	0,48	0,73
	ПФВК	1,9 – 6,0	0,8	0,62	1

Выводы

Рассмотренный класс сложных производных сигналов, полученный с применением предложенного метода на основе использования нелинейных криптографических сигналов, обладает, с одной стороны, структурными свойствами, аналогичными свойствам случайных (псевдослучайных) последовательностей, с другой, - требуемыми ансамблевыми и корреляционными свойствами.

Характеристики их авто- и взаимной функций корреляции таких сигналов не уступают характеристикам лучших с точки зрения корреляционных свойств дискретных последовательностей (М-последовательностей, множеств Голда и Касами, ансамблей Камалетдинова и др.). Кроме того, системы криптографических сигналов (КС) существуют и обладают указанными выше свойствами, для широкого спектра значений периода последовательностей. Также необходимо отметить особое свойство таких систем сигналов – возможность их восстановления в пространстве и времени с применением ключей и ряда других параметров, которые используются в процессе синтеза сигналов. Приведенные характеристики систем сигналов, синтезируемых с применением разработанного метода, позволяют говорить об улучшении качественных показателей функционирования телекоммуникационной системы: помехозащищенности и информационной безопасности.

Улучшение указанных показателей достигается, в частности, за счет возможности формирования, с применением полученного метода, больших ансамблей дискретных последовательностей практически любого периода с необходимыми (для тех или иных приложений системы) значениями боковых лепестков функций авто – взаимной и стыковой функции корреляции в периодическом и апериодическом режимах работы, а так же статистическими характеристиками корреляционных функций (КФ), не уступающих аналогичным характеристикам лучших, с точки зрения КФ, линейных классов сигналов. Указанное дает возможность повысить помехоустойчивость приема сигналов.

Разработаны математическое и программное обеспечение, реализующие предложенный метод и вычислительные алгоритмы синтеза систем сложных нелинейных дискретных криптографических сигналов, а также производных систем сигналов, для которых, в качестве производящих, используют КС. Программное и математическое обеспечение, полученное в ходе исследований, реализующее методы синтеза и исследования свойств систем нелинейных сигналов, в том числе ПСС, готово к возможному использованию в составе опытных образцов и элементов современных цифровых коммуникационных средств.

Список литературы

1. D.V. Sarvate, M.V. Pursley Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Pursley // IEEE Trans. Commun. Vol. Com 68-5, 1980.

2. Варакин Л. Е. Системы связи с шумападобными сигналами / Варакин Л. Е.-1985.-384 с.

3. Горбенко И.Д. Синтез систем сложных сигналов с заданными свойствами корреляционных функций для приложений многопользовательских систем с кодовым разделением абонентов / Замула А.А., Е.А. Семенко // Системи обробки інформації. – Х. ХУПС, 2014. – Вип. 9 (125).– С. 25 - 30.

4. Gorbenko I.D., Zamula A.A., Semenko Ye.A. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecom. and Radio Engineering. – 2016. – Vol. 75, Is. 2. – P. 169-178.

5. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Введ. 01–07–2015. – К.: Мінекономрозвитку України, 2015.

Надійшла до редколегії 16.02.2017

Рецензент: д-р техн. наук, проф. В.А. Краснобаєв, Харківський національній університет імені В.Н. Каразіна, Харків.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ СИНТЕЗУ ПОХІДНИХ СИСТЕМ СИГНАЛІВ ДЛЯ ДОДАТКІВ СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

О.А. Замула, В.Л. Морозов, Д.О. Семченко

Сформульовано вимоги до вибору систем складних сигналів - переносників даних для застосування в інформаційно-комунікаційних системах (ІКС), для яких пред'являються підвищені вимоги щодо забезпечення завадозахищеності, завадостійкості, скритності функціонування та інформаційної безпеки інформації. Представлені концептуальні засади синтезу нового класу складних сигналів криптографічних сигналів (КС). Обгрунтовується доцільність застосування КС в захищених ИКС, в тому числі, при формуванні похідних систем сигналів, з метою поліпшення показників завадозахищеності, завадостійкості, скритності функціонування та інформаційної безпеки інформації в захищених ІКС.

Ключові слова: *інформаційна безпека, скритність, завадозахищеність, система сигналів, похідні системи сигналів, широкосмугові системи.*

INFORMATION TECHNOLOGIES FOR SYNTHESIS OF DERIVED SIGNAL SYSTEMS FOR APPLICATIONS OF MODERN INFORMATION AND COMMUNICATION SYSTEMS

A.A. Zamula, V.L. Morozov, D.O.Semchenko

Requirements are formulated for the choice of complex signal systems - data carriers for use in information and communication systems (ICS), for which high demands are made for ensuring noise immunity, noise immunity, stealth operation and information security of information. Conceptual bases of synthesis of a new class of complex signals of cryptographic signals (CS) are presented. The expediency of using CS in protected TSS, including when generating derivative signal systems, for the purpose of improving the noise immunity, noise immunity, stealth performance and data security in protected IKS is grounded.

Keywords: *Information security, stealth, noise immunity, signal system, signal system derivatives, broadband systems.*