УДК 004.0561

Актуальные проблемы в построении сигнального обеспечения для имитостойких систем связи

А. Л. Лобков
Пермский государственный национальный исследовательский университет
Россия, 614990, г. Пермь, ул. Букирева, 15
armando.lobkov@yandex.ru; 89026444152

Проводится анализ построения сигнального обеспечения на основе фазоманипулированных сигналов, используемых в имитостойких системах передачи информации ограниченного доступа. Раскрываются основные недостатки применяемого сигнального обеспечения, в результате которых не обеспечивается защита сообщений от расшифровки в случае применения злоумышленником современных технических средств разведки и обработки информации ограниченного доступа. На основе полученных заключений сформулированы требования, предъявляемые к сигнальному обеспечению, позволяющие не допустить раскрытия построения кодового словаря, используемого в системах закрытой связи.

Ключевые слова: *линейные рекуррентные последовательности максимальной длины (ЛРПМ); линейные рекуррентные последовательности с трехуровневыми взаимокорреляционными функциями (ЛРПТ).*

DOI: 10.17072/1993-0550-2019-1-70-73

Известно, что для создания помехозащищенной на уровне сигналов системы связи необходимо использовать сложные фазоманипулированные (ФМ) сигналы, имеющие большой объем ансамблей V_x. Пределы любого большого ансамбля сложных сигналов определяются полным кодом, представляющим собой всю совокупность сигналов данного класса при заданном алфавите символов и числе символов в сигнале, где алфавит символов – это число различных символов, из которых состоит данный сигнал.

Различие сложных сигналов, принадлежащих данному ансамблю, реализуется за счет их отличия по форме. Поэтому для организации связи между несколькими абонентами с использованием сложных сигналов форма сигналов должна быть выстроена так, чтобы свести к минимуму взаимные помехи при их совместной работе в общей полосе частот, а также обеспечить заданный уровень конфиденциальности (скрытности) передаваемой информации.

Уровень взаимных помех, обусловленный неортогональностью сложных сигналов, в значительной степени зависит от их корреляционных свойств. Поэтому, помимо требования к объему ансамбля, при выборе систем сложных сигналов необходимо предъявлять жесткие требования к их уровню взаимной корреляции.

В настоящее время наиболее изучены и находят применение в системах закрытой сотовой связи (а также спутниковых системах персональной радиосвязи) ансамбли сложных фазоманипулированных сигналов линейной формы: линейные рекуррентные последовательности максимальной длины (ЛРПМ) или *М*-последовательности, а также линейные рекуррентные последовательности с трехуровневыми взаимокорреляционными функциями (ЛРПТ), получившие название *последовательности Голда.*

Характеристика ансамблевых и корреляционных свойств ЛППРМ рассмотрены в [1]. Правило формирования ЛРПМ может быть записано в виде следующего рекуррентного уравнения:

$$C_{i+1} = \sum_{k=1}^{n} \alpha_k C_{i+1-k}; \qquad (1)$$

где: $C_i = \{0,1\}$ – элементы ЛППРМ; α_k – коэффициенты при степенях примитивных неприводимых полиномов степени n, равные либо нулю, либо единице. При специально подобранных $\alpha_к$ рекуррентная формула (1) обеспечивает получение последовательностей максимальной длины, содержащих 2^n –1 элементов. База ЛРПМ, как и любого фазоманипулированного сигнала, равна

$$B = T / \tau_u = N_{фм}, \qquad (2)$$

где: τ_u – длительность одного временного дискрета;

T – период сигнала;

$N_{фм} = 2^n - 1$ – число элементов ЛРПМ.

Объем ансамблей M-последовательностей определяется количеством примитивных неприводимых полиномов заданной памяти n: его величина равна

$$V_{лрпм} = \varphi(N_{фм}) / n, \qquad (3)$$

где: $\varphi(x)$ функция Эйлера.

Величина максимальных пиков взаимокорреляционных функций (ВКФ) ЛРПМ определяется соотношением

$$R_{\max} = (1,4 \div 5) / \sqrt{N_{фм}}. \qquad (4)$$

Последовательности Голда (ЛРПТ) могут быть образованы путем относительного циклического сдвига двух исходных M-последовательностей и их сложения по модулю 2 [1]. Сочетание M-последовательностей, которые могут быть использованы для образования последовательностей Голда, выбираются с помощью таблиц [1]. Объем ансамбля, состоящего из последовательностей Голда, определяется по формуле

$$V_{лрпт} = N_{фм} + 2. \qquad (5)$$

Если последовательности построены по методу Голда, то их периодические ВКФ являются трехуровневыми, причем величина максимального пика ВКФ для последовательностей Голда в 2 раза больше, чем для ЛРПМ.

Рассмотренные особенности ансамблей и корреляционных свойств ЛРП позволяют выявить их недостатки.

Количество различных правил образования ЛРП, определяющих величину объема ансамбля при заданных корреляционных свойствах, ограничено числом примитивных непредвидимых полиномов заданной памяти n, причем для ЛРПМ, даже в наилучшем случае, когда $N_{фм}$ – простое число. Объем ансамбля в n раз меньше базы сигнала, а для ЛРПТ объем ансамбля лишь сравним с базой сигнала, поэтому, используя ЛРП, очень трудно выполнить требование по обеспечению должного уровня имитостойкости. В защищаемых радиоканалах требуется обеспечение уровня имитостойкости от 10^{-6} до 10^{-15}. Чтобы выполнить это требование необходимо применить ансамбли ЛРПТ с $B \geq 10^6$, так как только в этом случае вероятность раскрытия сложного сигнала злоумышленником будет меньше 10^{-6}. Применение сигналов с такими большими базами влечет за собой значительное усложнение аппаратуры формирования и обработки сигналов, вследствие чего не всегда осуществимо на практике.

Особенно серьезным недостатком ЛРПМ и ЛРПТ является то, что они не обеспечивают должную защиту сообщений от расшифровки. В [1] показано, что если известен сегмент ЛРПМ, содержащий $2^n - 1$ двоичных символов, то этого достаточно для расшифровки всех оставшихся элементов.

Действительно из формулы (1) следует, что для нахождения коэффициентов $\alpha_к$, которые задают номера отводов в цепи обратной связи генератора M-последовательности, необходимо решить следующую систему уравнений следующего вида:

$$\begin{cases} C_к = \alpha_1 C_{к-1} + \alpha_2 C_{к-2} + \ldots + \alpha_n C_{к-n}; \\ C_{к+1} = \alpha_1 C_к + \alpha_2 C_{к-1} + \ldots + \alpha_n C_{к-n+1}; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ C_{к+n-1} = \alpha_1 C_{к+n-2} + \alpha_2 C_{к+n-3} + \ldots + \alpha_n C_{к-1}. \end{cases} \qquad (6)$$

В этой системе неизвестными являются элементы $\alpha_к$, поэтому для того чтобы система (6) имела единственное решение, необходимо знать сегмент M-последовательности, состоящий из элементов, $C_{к-n}, C_{к-n+1}, C_{к-n+2}, \ldots, C_{к+n-1}$,

т.е. необходимо перехватить сегмент длиной $2_n - 1$.

Для расшифровки структуры последовательностей Голда необходимо решить систему уравнений, содержащую в два раза больше неизвестных то есть в этом случае необходим сегмент, содержащий $4_n - 1$ элементов. Это позволяет злоумышленнику раскрыть структуру последовательности по ее сегменту. При использовании современных быстродействующих ЭВМ задача раскрытия структуры *М*-последовательностей и производных от них последовательностей может быть решена в реальном масштабе времени для сигналов с достаточно большими базами.

Таким образом, при использовании современной быстродействующей ЭВМ задача раскрытия структуры ЛРПМ и ЛРПТ может быть решена в достаточно короткие сроки, даже если база ЛРП составляет $1{,}2*10^{30}$, что позволит злоумышленнику получать оперативно любую информацию ограниченного доступа передаваемою по закрытой сотовой связи или спутниковой системы персональной радиосвязи.

В дальнейшем устойчивость сложных сигналов к раскрытию структуры будем характеризовать сигнальной скрытностью

$$S_c = l / N_{фм}, \qquad (7)$$

где l – количество символов, которые необходимо вычислить, чтобы однозначно определить оставшиеся $N_{фм} - l$ символов.

Из формулы (7) видно, что сигнальная скрытность ЛППРМ определяется соотношением

$$S_{лрпм} = (2n-1)/(2^n - 1), \qquad (8)$$

а ЛРПТ –

$$S_{лрпт} = (4n-1)/(2^n - 1), \qquad (9)$$

поэтому с ростом базы сигналов сигнальная скрытность ЛРП становится сколь угодно малой величиной. Это и позволяет утверждать, что ЛРП легко поддаются расшифровке.

Таким образом, проведенный анализ радиоканалов со сложными ФМ сигналами показывает, что они недостаточно защищены на уровне сигналов как с точки зрения имитостойкости, так и скрытности, что приводит к раскрытию структуры сигнала и получению из него интересующей информации.

Рассмотрим, каким же основным требованиям должны удовлетворять ансамбли сложных сигналов при их использовании в системах закрытой сотовой связи и спутниковых системах персональной радиосвязи.

Во-первых, сложные сигналы должны в отличие от ЛРП обладать устойчивостью к раскрытию структуры. Для этого закон формирования каждого из сигналов системы должен быть таким, чтобы структура сигнала не могла быть раскрыта за время, меньшее одного периода сигнала. В этом случае сигнальная скрытность будет максимальной. Данное требование может быть выполнено только в том случае, если закон формирования сложного сигнала является псевдослучайным, т.е. при перехвате любого числа символов ($l=N_{фм}$) кроме перебора не должно существовать однозначного решения относительно закона формирования сложного сигнала, что возможно при использовании сложных сигналов с нелинейной структурой.

Во-вторых, объем ансамбля сложных сигналов должен быть таким, чтобы исключить многократное использование одних и тех же кодовых словарей за цикл радиосвязи.

Самые эффективные регулярные алгоритмы построения систем сложных сигналов позволяют синтезировать ансамбли, объем которых при приемных корреляционных свойствах соизмерим с базой сигнала. Поэтому требования по обеспечению имитостойкости, скрытности, а также помехоустойчивости источника сигналов труднореализуемы на практике ввиду чрезмерной сложности устройств формирования и обработки.

Однако, если использовать динамический режим функционирования радиоканалов, когда соответствие информационных символов сложных сигналов изменяется с течением времени по непредсказуемому закону, то требования по имитостойкости, скрытности, а также по помехоустойчивости источника сложных сигналов можно выполнить, используя ансамбли сложных сигналов с нелинейной структурой сравнительно небольшого объема (например, псевдослучайные последовательности *де Брейна*).

В этом случае количество априорно известных злоумышленнику сложных сигналов при условии, что соответствие m–бит 2^m сигналам изменяется с периодичностью mT, определяется соотношением

$$V_x = QL; \qquad (10)$$

где: Q – число ансамблей (систем) данного класса сложных сигналов, существующих при заданной длительности кодовой последовательности;

L – объем ансамбля, обеспечивающий заданные взаимокорреляционные свойства сложных сигналов.

Формула (10) будет справедлива, если сигналы сменяемых ансамблей являются слабо корреляционными между собой.

Обеспечение этого условия возможно, если с большой вероятностью любая, случайным образом выбранная из полного кода пара сложных сигналов имеет допустимые взаимокорреляционные свойства.

В-третьих, ансамбли сложных сигналов должны обеспечивать устойчивую работу систем связи при возникновении непреднамеренных помех, т.е. быть инвариантными к воздействию взаимных помех, возникающих из-за работы других радиоэлектронных средств. Приемное устройство должно гарантировать надежный прием информации, если отношение мощности сигнала к мощности помехи находится в пределах $P_c/P_п \geq -40$ дБ.

И, наконец, при выборе систем сложных сигналов необходимо учитывать простоту реализации их устройств формирования и обработки, т.е. необходимо использовать такие сложные сигналы, которые можно было бы формировать и обрабатывать в реальном масштабе времени, используя современную элементную базу.

Таким образом, основные требования по обеспечению должного уровня имитостойкости и скрытности сводятся к выбору и детальному исследованию такого класса сложных сигналов, на основе которого можно регулярным образом производить формирование большого разнообразия систем сложных сигналов с нелинейной структурой, обладающих заданными ансамблями, корреляционными и структурными свойствами. Кроме того, устройства обработки таких сигналов должны быть инвариантны к воздействию комплекса непреднамеренных помех и технически достаточно просто реализуемы при использовании современной элементной базы.

Список литературы

1. *Варакин Л.Е.* Помехоустойчивость ШИМ–ШПС и ЧМ–ШПС. Радиотехника. 1983. № 5.
2. *Ипатов В.П., Камалетдинов Б.Ж., Самойлов И.М.* Исследование корреляционных свойств *M*-последовательностей и ансамблей. Радиотехника и электроника. Т. 34, №2. 1989.
3. *Кругликов Н.В., Крейнделин В.Б.* Ансамбли нелинейных псевдослучайных последовательностей с хорошими корреляционными свойствами. Радиотехника. № 8. 1994.
4. *Мазурков М.И.* Системы широкополосной связи: учеб. пособие для студ. вузов. Наука и техника, 2009. 344 с.

Current problems in alarm maintenance construction for spoofing resistant communications systems

A. L. Lobkov
Perm State University; 15, Bukireva st., Perm, 614990, Russia
armando.lobkov@yandex.ru; 89026444152

The paper analyzes construction of alarm maintenance based on PSK signals used in spoofing resistant systems of transferring information with restricted access. The paper shows the main limitations of the applied alarm maintenance, which result in failure to provide protection of messages against decoding in case when a malefactor uses modern means of investigating and processing restricted access information. Based on the conclusions received, there are defined the requirements to alarm maintenance making it possible to avoid disclosure of the code dictionary used in privacy communications systems.

Keywords: *maximum length linear recurrence sequence; linear recurrence sequence with 3-level cross-correlation functions.*