УДК 621.391.82

И. И. СНЫТКИН, канд. техн. наук

МЕТОД ГЕНЕРИРОВАНИЯ КОДО-ДИСКРЕТНО-ЧАСТОТНЫХ СИГНАЛОВ ДЛЯ ИМИТОСТОЙКИХ МНОГОКАНАЛЬНЫХ СИСТЕМ СВЯЗИ

В современных системах связи специального назначения, использующих сложные сигналы, важное значение имеет обеспечение скрытности, имитостойкости связи [1—5], понимая под этим способность системы противостоять раскрытию структуры сигналов и их имитации за счет изменения объема используемых сложных сигналов, формируемых на основе идентичных элементов, изменения различных параметров используемых сигналов и др. [2; 4; 5]. В настоящее время широкое распространение в качестве сложных сигналов получили линейные рекуррентные последовательности (ЛРП): последовательности немаксимальной и максимальной длины, сегментные последовательности, последовательности Гоулда, ЛРД-коды, что обусловлено фактом их простого генерирования посредством регистров сдвига с линейными обратными связями [1; 3; 4]. Однако использование ЛРП не обеспечивает необходимые для специальных систем скрытности, имитостойкости связи, так как для ЛРП существуют эффективные методы раскрытия структуры и имитации [2; 4]; ЛРП существуют для ограниченного числа длительностей и имеют небольшую мощность кодирования, что не позволяет создавать большие объемы сигналов произвольных длительностей [1—4]. Поэтому в теории и практике систем сигналов существует весьма актуальная задача: создание устройств, обеспечивающих генерирование широких классов и больших объемов систем имитостойких скрытных сигналов, обладающих при этом и высокими ансамблевыми характеристиками [1—4].

К перспективным имитостойким скрытным системам сигналов относятся кодо-дискретно-частотные сигналы (КДЧС), потенциальные возможности которых в этой связи весьма высокие. Так, в структурных свойствах КДЧС объединены, во-первых, все известные свойства ДЧС [1; 3] (простая реализация большой базы сигнала, получение лучшей помехоустойчивости относительно некоторых видов организованных помех и значительное ослабление действия мешающих сигналов, минимальная взаимная коррекция, минимальный уровень шумов ортогональности при синхронной работе и др.), во-вторых, использование кодовой манипулирующей функции КДЧС, отвечающей за состав, форму КДЧС, длительность составляющих элементов и самого КДЧС, число и номинальные значения используемых частот-элементов, позволяет создавать практически не ограниченные по величине объема V словари ДЧС всевозможных длительностей, форм и видов.

Если вопросы эффективного формирования (или генерирования) высокостабильных элементов ДЧС являются в теории и практике решенными [1;3], то обеспечение формирования, с одной стороны, систем псевдослучайных кодовых манипулирующих функций и в целом генерирования систем КДЧС представляет собой актуальную научно-техническую задачу, способы решения которой приведены, например, в работе [7], где в качестве структурных свойств кодовых манипулирующих функций КДЧС используются свойства и закономерности расширенных полей Галуа и их элементов, в частности, цикличность последовательности элементов полей, зависимость структуры элементов поля от выбранного первообразного элемента и др. [6]. Ниже на примере работы [7] рассматривается процесс генерирования имитостойких систем КДЧС.

Генерирование систем КДЧС. На рис. 1 представлена функциональная схема устройства; на рис. 2 — функциональная схема блока формирования дискретно-частотных сигналов; на рис. 3 — функциональная схема блока распределения импульсов.

Устройство содержит блоки $1_1 - 1_{n-1}$ умножения по модулю p, блоки $2_1 - 2_n$ формирования частичных произведений, сумматоры

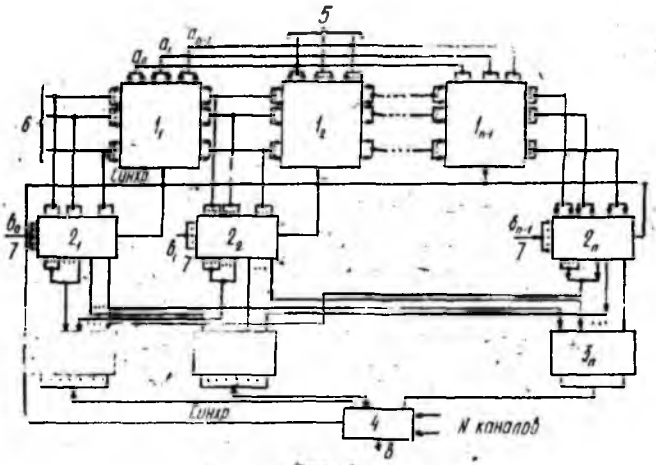

Рис. 1

$3_1 - 3_n$ по модулю p, блок *4* формирования дискретно-частотных сигналов, вход *5* производящего полинома, первую группу входов *6* произвольных элементов полей Галуа $GF(p^n)$, вторую группу входов *7* произвольных элементов полей Галуа $GF(p^n)$ и выход *8* устройства.

Блок формирования дискретно-частотных сигналов содержит дешифратор *9*, блок *10* распределения импульсов, генератор *11* тактовых импульсов, делитель *12* частоты импульсов, первый элемент ИЛИ *13*, элемент И *14*, аналого-цифровой преобразователь (АЦП) *15*, генератор $16_1 - 16_n$ высокостабильных частот, элементы И $17_1 - 17_n$ группы, второй элемент ИЛИ *18*, блок *19* уплотнения сообщений.

Блок уплотнения сообщений содержит генератор *20* тактовых импульсов, кольцевой сдвигающий регистр *21*, элементы МИ $22_1 - 22_n$ и элемент ИЛИ *23*.

Блок распределения импульсов содержит генератор *24* тактовых импульсов, элементы И $25_1 - 25_n$, счетчик *26* и регистр *27*.

Устройство работает следующим образом. Модульные блоки 1_i осуществляют умножение полинома-элемента A^k-го на x и приведение

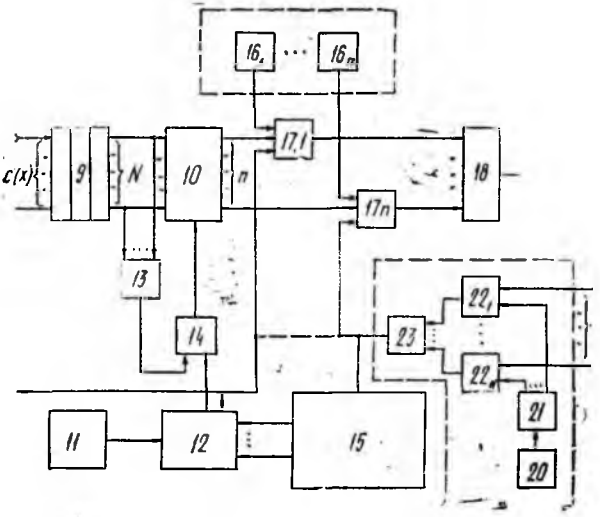

Рис. 2

результата по modd $(a(x), p)$, тем самым осуществляя получение элемента (A^{k+1})-го. Блоки 2_i формирования частичных произведений осуществляют частичное произведение $A(x) \cdot (B_i \cdot x^i)$. Сумматоры 3_i по модулю p осуществляют суммирование по модулю p таким образом, что на выходах сумматоров *3* по модулю p отображаются коэффициенты соответственно C_0, C_1, ..., C_{n-1} полинома, представляющего собой результат умножения полиномов элементов A (x) и B (x) поля $GF(p^n)$. Последовательность кодов коэффициентов поступает на блок *4* формирования ДЧ сигналов, где происходит образование сложных ДЧС. В основе функционирования блоков *1*, *2*, *3* лежит следующее рекуррентное правило: коэффициенты $A_0^{k+1} - A_{n-1}^{k+1}$ каждого последующего полинома-элемента A^{k+1} поля $GF(p^{n_1})$ вычисляется с использованием коэффициентов $A_0^k - A_{n-1}^k$ предыдущего полинома элемента A^k и коэффициентов $(a_0 - a_{n_1})$ первообразного полинома $a(x)$ по правилу

$$A_0^{k+1} \equiv A_{n-1}^k \cdot a_0 \pmod{p};$$

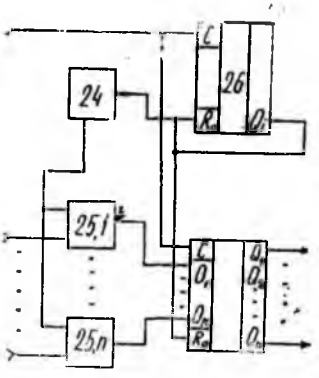

Рис. 3

$$A_j^{k+1} \equiv A_{n-1}^k a_j + A_{j-1}^k \pmod{p};$$
$$j = 0,\ 1,\ 2,\ \ldots,\ n-1.$$

Цифровой код с выходов АЦП *15* поступает на первые управляющие входы делителя *12* с переменным коэффициентом деления (ДПКД).

На второй вход ДПКД *12* подаются импульсы с генератора *11* тактовых импульсов. ДПКД *12* в соответствии с поступившим на его вход кодом изменяет коэффициент деления и выдает последовательность импульсов с измененным в соответствии с кодом периодом их следования. Эти импульсы проходят через элемент И *14*, открытый сигналом с выхода элемента ИЛИ *13*, на входы распределителя *10* через его второй вход в такой последовательности, которая определяется номером входа блока распределения, на котором существует сигнал с дешифратора *9*. Таким образом, в зависимости от того, на каком из первых входов блока *10* распределения существует импульс с выхода дешифратора *9*, будет изменяться последовательность распределения импульсов, поступающих на второй вход блока *10* распределения. С выхода блока *10* распределения импульсы поступают на первые входы элементов И *17*, на вторые входы которых подается сигнал с генераторов *16* высокостабильных частот, на третьи — сигнал с выхода блока *19* уплотнения сообщений.

Каждому информационному импульсу на выходе блока *19* управления сообщений соответствует определенный коэффициент на входе дешифратора *9*, а следовательно, и определенный порядок распределения импульсов с выхода ДПКД *12* по выходам блока *10* распределения.

Таким образом, элементы И *17* открываются поочередно в порядке, определенном для каждого информационного импульса, пропуская на выход *8* одну из частот генераторов *16* высокостабильных частот. Очередность открывания элементов И *17* определяет структуру ДЧ сигнала. Коэффициент C_i в параллельном коде поступает с выходов сумматоров *3* по модулю p на входы 1, 2, ..., k дешифратора *9*, который последовательно по тактам на каждый пришедший коэффициент C_i выдает сигнал только на одном из своих выходов 1, 2, ..., N. Этот сигнал является управляющим для работы блока *10* распределения и одновременно через элемент ИЛИ *13* поступает на первый вход элемента И *14*. С выходов АЦП *15* снимается цифровой код, который поступает на управляющие входы ДПКД *12*, на другой вход *2* которого поступают импульсы с генератора *11*. С выхода ДПКД *12* на второй вход элемента И *14* поступают импульсы с измененным в зависимости от длительности импульса с выхода блока *19* периодом их следования. Эти импульсы проходят через открытый элемент И *14* на вход блока *10* распределения в такой последовательности, которая определяется номером входа, на котором существует единичный сигнал от дешифратора *9*. Эта последовательность импульсов с выходов блока *10* распределения управляет работой элементов И *17* по их второму входу, на первый вход которых подаются высокостабильные частоты от генераторов *16*, на третьи входы элементов И *17* подается последовательность

информационных импульсов с выхода блока *19* уплотнения. Выходы элементов И *17* соединены с входами элемента ИЛИ *13*, на выходе которого будет сформирован ДЧС, структура его определяется очередностью открывания элементов И *17*, которая, в свою очередь, зависит от поступившего на входы дешифратора *9* коэффициента C_i.

Если увеличивается длительность информационной посылки T, изменяется цифровой код, поступающий с выходов АЦП *15* на первые управляющие входы ДПКД *12*. Соответственно этому коду изменяется коэффициент деления ДПКД *12*, а следовательно, изменяется (в данном случае увеличивается) период следования тактовых импульсов с выхода ДПКД *12* через элемент И *14* на второй вход блока распределения, а значит, увеличиваются длительности ДЧ сигнала и элемента ДЧ сигнала.

Таким образом, на выходе *8* устройства формируется последовательность дискретных частотных сигналов в соответствии с последовательностью параллельных двоичных кодов коэффициентов C_0, C_1, ..., C_{n-1}. Структура ДЧ сигнала определяется коэффициентом C_i, а длительность ДЧ сигнала T и длительность элемента ДЧС Δt — длительностью информационной посылки.

Итак, использование структурных свойств конечных полей Галуа для генерирования имитостойких систем КДЧС, в частности, манипулирующих функций КДЧС, является одним из возможных путей решения данной задачи. Применение с этой целью других закономерностей, известных в алгебре, может привести к новым оригинальным решениям указанной задачи.

Список литературы: 1. *Варакин Л. Е.* Теория систем сигналов. М., 1978. 304 с. 2. *Диффи У., Хэлман М. Э.* Защищенность и имитостойкость. Введение в криптографию // Тр. инж. Ин-та. по электротехнике и радиоэлектронике. 1979. Т. 67, № 3. С. 48—59. 3. *Варакин Л. Е.* Системы связи с шумоподобными сигналами. М., 1985. 384 с. 4. *Диксон Р. К.* Широкополосные системы : пер. с англ. / Под ред. В. И. Журавлева. М., 1979. 302 с. 5. *Каневский З. Н.* Энтропийная оценка скрытности радиопередачи // Радиотехника. 1980. № 4. С. 32—34. 6. *Постников М. М.* Теория Галуа. М., 1963. 218 с. 7. *А. с. 1334143 СССР, МКИ*[3]. Устройство для умножения произвольных элементов расширенных полей Галуа $GF(p^n)$ / И. И. Сныткин // Открытия. Изобретения. 1987. № 32. С. 189.

Поступила в редколлегию 19.10.88