УДК 621.392.82

И. И. СНЫТКИН

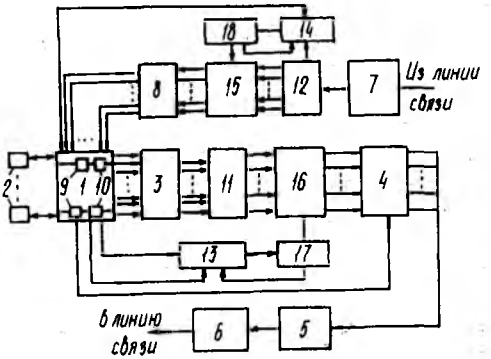
СКРЫТНАЯ ИМИТОСТОЙКАЯ ШИРОКОПОЛОСНАЯ СИСТЕМА СВЯЗИ С ПРОГРАММНО-ИЗМЕНЯЕМЫМИ КОДОВЫМИ СЛОВАРЯМИ ОПТИМАЛЬНЫХ ДИСКРЕТНЫХ СИГНАЛОВ НЕЛИНЕЙНОЙ СТРУКТУРЫ

Широко известно, что использование в системах связи с ШПС оптимальных дискретных сигналов в виде М-последовательностей, ЛРД-кодов, последовательностей Гоулда и других разновидностей линейных рекуррентных последовательностей (ЛРП) не обеспечивает скрытности, имитостойкости передачи информации вследствие того, что для ЛРП существуют эффективные и простые алгоритмы раскрытия их структуры и имитации, если известны $(2n+1)$ символов ЛРП (длительность ЛРП $L=2^n-1$) [1; 2]. В работе [1] прямо указывается, что обеспечение скрытности, имитостойкости передачи информации возможно только при использовании оптимальных дискретных сигналов нелинейной структуры — нелинейных рекуррентных последовательностей (НЛРП), которые не генерируются регистрами сдвига с линейными обратными связями (РС с ЛОС), за исключением вырожденного вида НЛРП в виде «полных кодовых колец», которые генерируются РС с ЛОС с добавлением одной нелинейной связи в виде элемента И [2]. К таким НЛРП относятся характеристические коды, коды квадратичных вычетов, составные и производные коды на их основе, свойства и правила построения которых приведены в работе [3]. Для них не разработаны или существенно затруднены алгоритмы раскрытия структуры и имитации [1], они существуют практически для произвольных длительностей $L=p$, $p-1$, p^n-1, где p — простое число, обладает большой (намного большей чем у ЛРП) мощностью кодирования, что позволяет создавать на их основе кодовые словари большого объема V, в том числе при фиксированной L (для НЛРП $V \gg L$ при $L=\text{const}$, тогда как для ЛРП $V \geqslant L$ при $L=\text{const}$) [2]. В работе [4] показано, что скрытность (различных видов) радиопередачи в значительной мере зависит от объема V сменяемых параметров, в нашем случае — сменяемых кодовых слов, т. е. от объема V используемого кодового словаря. Например, как следует из работы [4], скрытность объема сменных кодовых слов оценивается как $S_v=\log V$, а время, необходимое для раскрытия S_v, $T_v=S_v \cdot \delta$, где δ — время, необходимое для раскрытия одного параметра (в нашем случае — одной кодовой формы) с первой попытки.

Как следует из выше указанного, $\delta_{\text{НЛРП}} \gg \delta_{\text{ЛРП}}$, а $V_{\text{НЛРП}} \gg V_{\text{ЛРП}}$ даже при фиксированных и близких по значению L. Таким образом, можно утверждать, что использование НЛРП, выбираемых и сменяемых из объема V кодового словаря НЛРП, само по себе уже обеспечивает высокую скрытность передачи информации. Если же

при этом предполагать, что смена НЛРП в процессе работы будет производиться по некоторому рандомизированному или программно-изменяемому закону, то можно утверждать, как следует из работ [1; 4], что будет обеспечена и имитостойкость передачи информации.

Реализация на практике данных предпосылок требует разработки определенных методов, принципов построения и функционирования подсобных систем в виде соответствующих технических решений. Ниже рассматривается один из эффективных вариантов построения и функционирования такого рода систем связи с ШИС на примере работы [5].



Построение и функционирование системы. На рисунке дана структурная электрическая схема системы.

Система содержит блок *1* управления, распределителя *2* импульсных серий магистральных линий связи и абонентского комплекта, блок *3* статистического уплотнения, кодово-адресную матрицу *4*, блок *5* преобразования, передатчик *6*, приемник *7*, блок *8* разделения каналов магистральных линий связи, блоки *9* асинхронного сопряжения, схемы *И 10*, блок *11* образования группы каналов, блок *12* выделения каналов, генераторы *13*, *14* рекуррентной последовательности, коммутаторы *15*, *16*, дешифраторы *17*, *18*.

Система работает следующим образом.

Блок *1* осуществляет управление и коммутацию оконечных абонентских комплектов к передающей и приемной частям устройства, управление и коммутацию выделенных в приемной части каналов на передачу (режим ретрансляции). В результате этого в блок *3* по раздельным каналам поступают информационные посылки. В последнем производится статистическое уплотнение передаваемой информации.

В блоке *11* осуществляется параллельный опрос групп каналов, каждая из которых содержит k каналов, и каждому состоянию каждой группы ставится в случайное соответствие, установленное к данному моменту времени посредством коммутатора *16*, кодово-адресная матрица *4*. С кодово-адресной матрицы *4* производится параллельное считывание кодово-адресных групп на вход блока *5*, который совместно с передатчиком *6* обеспечивает последовательную передачу кодово-адресных групп в магистральную линию связи. Кроме того, посредством блока *1*, генератора *13*, дешифратора *17*, коммутатора *16*, кодово-адресной матрицы *4* осуществля-

ется по псевдослучайному закону во времени, устанавливаемому оператором на данный сеанс связи, перекоммутация соответствий состояний групп каналов блока *11* кодово-адресным группам кодово-адресной матрицы *4*.

Из линии связи кодово-адресные группы поступают в приемник *7*, а затем в блок *12*, в котором каждой кодово-адресной группе ставится в соответствие определенное состояние группы каналов. А каждому состоянию каждой группы каналов ставятся в случайное соответствие, совпадающее с соответствием на передающей стороне данной линии связи и установленное к данному моменту времени посредством коммутатора *15* на основании принимаемого и обрабатываемого блоком *12* сигнал-маркера о перекоммутации, входы блока *8*, который разделяет каналы и восстанавливает в них информационные посылки, которые поступают на оконечные абонентские комплекты или в передающую часть системы в режиме ретрансляции. Кроме того, посредством блока *1* управления коммутатора *15*, генератора *14*, дешифратора *18* осуществляется по псевдослучайному закону во времени, устанавливаемому оператором на данный сеанс связи на основании сигнала-маркера о перекоммутации, принимаемого и выделяемого блоком *12*, рандомизированная перекоммутация, совпадающая с перекоммутацией на передающей стороне данной линии связи соответствий между состояниями групп каналов блока *12* и входами блока *8*. Сигнал-маркер о перекоммутации представляет собой кодово-адресную группу кодово-адресной матрицы *4*, обладающую наилучшими авто- и взаимокорреляционными свойствами, что должно обеспечивать наименьшую вероятность ее ошибочного приема.

Перед началом сеанса связи в момент t_1 оператор для каждой линии связи устанавливает посредством блока *1* одинаковые (для определенной линии связи) начальные состояния генераторов *13*, *14*, а также псевдослучайный во времени закон моментов рандомизированной перекоммутации соответствий между состояниями групп каналов и кодово-адресными группами, согласованный с работой системы в целом таким образом, что выдача сигналов о перекоммутации — сигнала считывания, поступающего из блока 1 на вход генератора *13* и сигнала управления с выхода блока *1* на управляющий вход кодово-адресной матрицы *4* для выдачи маркера перекоммутации — осуществляется только после выдачи информационной кодово-адресной группы из кодово-адресной матрицы *4*.

После этого оператор в момент t_2 выдает сигнал о начальной установке коммутации — сигнал «начального считывания» — по выходу блока *1* и сигнал управления с выхода блока *1* на управляющий вход кодово-адресной матрицы *4*, обеспечивающий выдачу ею кодово-адресной группы.

Затем оператор в момент t_2 выдает сигнал о начальной установке коммутации — сигнал «начального считывания» — по выходу блока *1* и сигнал управления с выхода блока *1* на управ-

ляющий вход кодово-адресной матрицы *4*, обеспечивающий выдачу кодово-адресной группы маркера перекоммутации из кодово-адресной матрицы *4* в период t_3—t_5, считывание начально-установленной рекуррентной последовательности из генератора *13* в дешифратор *17* в период t_3—t_4 и следующие за эти дешифрование рекуррентной последовательности и выдачу из дешифратора *17* на управляющий вход коммутатора *16* в период t_4—t_5 для установки начального соответствия между состояниями групп каналов и кодово-адресной матрицы *4*.

В момент t_4 из дешифратора *17* на вход генератора *13* поступает сигнал о сдвиге начальной рекуррентной последовательности на один такт, тем самым формируется новая рекуррентная последовательность. На приемной стороне данной линии связи в момент t_2—t_3 кодово-адресная группа маркера перекоммутации обрабатывается блоком *12* в сигнал «начального считывания», поступающий с управляющего выхода блока *12* на вход генератора в момент t_3 и обеспечивающий считывание начально-установленной (для данной линии связи) рекуррентной последовательности из генератора *14* на вход дешифратора *18* в период t_4—t_5, дешифрирование рекуррентной последовательности и выдачу из дешифратора *18* на управляющий вход коммутатора *15* в период t_5—t_6 сигнала для установки начального (адекватного с передающей стороной данной линии связи) соответствия между состояниями групп каналов блока *12* и входами блока *8*, а также выдачу в момент t_5 из дешифратора *18* на вход генератора *14* сигнала о сдвиге начальной рекуррентной последовательности на один такт, тем самым формируется новая рекуррентная последовательность, идентичная передающей стороне.

В последовательности периодов (t_7—t_8) —-(t_9—t_{10}) на передающей стороне из блока *11* на начально-установленные ранее коммутатором *16* входы кодово-адресной матрицы *4* поступают сигналы о состояниях групп каналов ($1^{\text{п}}$—$i^{\text{п}}$), которые в кодово-адресной матрице *4* преобразуются в определенные информационные кодово-адресные группы, выдаваемые в периоды (t_8—t_9) — —(t_{11}—t_{12}) на блок *5* и далее на передатчик *6*. В момент t_{12} на вход генератора *13* поступает сигнал считывания, а на управляющий вход кодово-адресной матрицы *4* — сигнал о выдаче маркера перекоммутаций. В период t_{13}—t_{15} кодово-адресная матрица *4* выдает кодово-адресную группу маркера перекоммутации. В период t_{13}—t_{14} в дешифратор *17* из генератора *13* поступает рекуррентная последовательность, которая дешифруется и в период t_{14}—t_{16} выдается из дешифратора *17* на управляющий вход коммутатора *16* сигналом рандомизированной перекоммутаций соответствий между состояниями групп каналов и входами кодово-адресной матрицы *4*. После перекоммутации из блока *11* в период t_{17}—t_{18} через новую цепь соответствия, установленную коммутатором *16* на соответствующий данной коммутации вход кодово-адресной матрицы *4*, поступает следующий «$i+1$» сигнал о состоянии группы каналов, выдаваемый в период t_{18}—t_{19} соот-

ветствующей «$i+1$» информационной кодово-адресной группой из кодово-адресной матрицы *4*. В момент t_{14} из дешифратора *17* на вход генератора *13* поступает сигнал о сдвиге рекуррентной последовательности на один такт; тем самым формируется новая рекуррентная последовательность. В последующий период (t_{20}—t_{29})—t_{∞} динамика работы передающей стороны аналогична описанной.

На приемной стороне приходящая в последовательность моментов (t_7—t_8) — (t_{10}—t_{11}) последовательность 1 — i информационных кодово-адресных групп после приемника *7* поступает на блок *12*, а с него выдается последовательность ($1^{и}$ — $i^{и}$) сигналов в период (t_8 — t_9) — (t_{11} — t_{13}) о состоянии соответствующих групп каналов через начально-установленные коммутатором цепи соответствий на входы блока *8*. Приходящая в период t_{12}—t_{14} кодово-адресная группа маркера перекоммутации выделяется блоком *12* сигналом «считывания» на вход генератора *14* в момент t_{14}. В период t_{15}—t_{16} в дешифратор *18* из генератора *14* поступает рекуррентная последовательность, которая дешифруется и в период t_{16}—t_{18} выдается из дешифратора *18* на управляющий вход коммутатора *15* сигналом рандомизированной перекоммутации соответствий между состояниями групп каналов и входами блока *8*. После перекоммутации пришедшая в период t_{17}—t_{19} «i—1» информационная кодово-адресная группа выдается из блока *12* в период t_{19}—t_{20} по новой цепи соответствия, установленной коммутатором *15* соответствующим сигналом состояний группы каналов на соответствующий данной коммутации вход блока *8*. В момент t_{16} из дешифратора *18* на вход генератора *14* поступает сигнал о сдвиге рекуррентной последовательности на один такт. Тем самым формируется новая рекуррентная последовательность, идентичная новой рекуррентной последовательности на передающей стороне данной линии связи.

В последующий период (t_{21}—t_{30}) — t_{∞} динамика работы приемной стороны аналогична описанной.

Таким образом, построение и функционирование рассмотренной выше системы не исключает возможности использования и ЛРП. Однако в этом случае трудно обеспечивается лишь имитостойкость связи (причем только на период сеанса связи), скрытность же обеспечена не будет. Следовательно, высокая эффективность системы будет достигаться лишь при использовании кодовых словарей НРЛП.

Список литературы: 1. *Диксон Р. К.* Широкополосные системы: Пер. с англ./ Под. ред. В. И. Журавлева. М., 1979. 302 с. 2. *Варакин Л. Е.* Системы связи с шумоподобными сигналами. М., 1985. 384 с. 3. *Свердлик М. Б.* Оптимальные дискретные сигналы. М., 1975. 201 с. 4. *Каневский З. М.* Энтропийная оценка скрытности радиопередачи//Радиотехника. 1980. № 4. С. 31—35. 5. *А. с. 762208 СССР.* Устройство для уплотнения и коммутации каналов связи/И. И. Сныткин// Открытия. Изобретения. 1980. № 33. С. 296.

Поступила в редколлегию 17.06.88