Из теории чисел известно, что если период элемента a в поле GF(P) есть E (E — максимальный период элемента поля) и наибольший общий делитель (β, E) = 1, то период элемента $a^\beta = E = P - 1$, а значит a^β — первообразный элемент поля. Находя числа β, для которых выполняется условие (β E) = 1 и, возводя a в степень β, можно получить множество первообразных элементов поля GF(P). Общее число первообразных элементов $M = \varphi(P - 1)$, где $\varphi(\cdot)$ — функция Эйлера.

Для построения множества НП необходимо осуществлять расчет коэффициентов децимации, для которых выполняется условие (c, P — 1) = 1. Для расчета β и c взаимно простых с $P - 1$ может быть использован алгоритм Эвклида.

Число элементов НП выбирается в зависимости от требуемой величины частотной избыточности и характера ее реализации. Например, при ФМШПС величина L равна базе B используемого сигнала $L = B = \Delta f \cdot T_c$ **(6)**, где Δf — полоса частот, занимаемой ФМШПС; T_c — длительность сигнала.

В случае применения ППРЧ ФМ сигнала величина L также определяется из соотношения (6), однако в этом случае T_c — есть время изучения сложного сигнала на одной частоте. При этом величина $L = B$ выбирается из условия $B \geqslant B_{доп}$, где $B_{доп}$ — минимально допустимый выигрыш при обработке сигнала.

Список литературы: 1. *Свердлик М. Б.* Оптимальные дискретные сигналы. М., 1975. 200 с. 2. *Горбенко И. Д., Замула А. А.* Ускоренные алгоритмы формирования систем характеристических дискретных сигналов // Радиотехника. Вып. 84. С. 69—72. 3. *Горбенко И. Д., Замула А. А., Кулешов В. Л.* Корреляционные свойства систем характеристических дискретных сигналов // Радиотехника. Вып. 85. С. 96—100. 4. *Лидл Р., Нидеррайтер Г.* Конечные поля. В 2-х т.: Пер. с англ., М., 1988. Т. 2. 822 с.

Поступила в редколлегию 30.03.80

УДК 621.391.82

И. И. СНЫТКИН, канд. техн. наук

ГЕНЕРИРОВАНИЕ ИМИТОСТОЙКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДИСКРЕТНО-ЧАСТОТНЫХ СИГНАЛОВ

В системах связи со сложными сигналами все большее распространение получают дискретные частотные сигналы (ДЧС) вследствие ряда преимуществ по отношению к ФМ-оптимальным дискретным сигналам, а именно [1; 3]: простой реализацией большой базы сигнала, получением лучшей помехоустойчивости относительно некоторых видов организованных помех и значительным ослаблением действия мешающих сигналов, минимальной взаимной корреляцией, минимальным уровнем шумов ортогональности при синхронной работе и др. Однако к системам связи со сложными сигналами (особенно специального назначения) в настоящее время

стали предъявляться достаточно жесткие требования по защищенности и имитостойкости (криптоустойчивости) связи [2; 4; 5]. А эти требования традиционные, широко распространенные системы сложных сигналов (например, линейные рекуррентные последовательности — ЛРП, последовательности Гоулда, ЛРД-коды, ДЧС) не обеспечивают, так как для них существуют эффективные алгоритмы раскрытия структуры и имитации [4]. В этой связи весьма важным является нахождение таких научных методов и технических решений, которые позволяли бы, не лишая известные системы сигналов их преимуществ и положительных свойств, наделять их свойствами имитостойкости и скрытности.

Одним из таких методов является метод, основанный на обеспечении изменения вида, формы и состава ДЧС за счет изменения вида манипулирующей функции в процессе работы по некоторой программе. В данном случае манипулирующая функция (некоторая кодовая форма) непосредственно отвечает за вид, форму и состав ДЧС, состоящего, как известно, из некоторых частотных элементов, распределенных дискретно во времени. Таким образом, обычный ДЧС преобразуется в некоторую кодовую форму ДЧС или кодо-дискретно-частотный сигнал (КДЧС). Если при этом манипулирующие функции и весь процесс их изменения в процессе работы системы (программу работы) наделить свойствами имитостойкости и скрытности, то такие КДЧС будут эффективно решать указанную выше задачу. Одним из путей наделения КДЧС такими свойствами является использование в качестве структурных свойств кодовых манипулирующих функций — свойств и закономерностей конечных полей Галуа и последовательностей их элементов, в частности: цикличность и псевдослучайность последовательности элементов полей, зависимость структуры элементов поля и самой последовательности элементов поля от выбранного первообразного элемента и др. [6]. Ниже рассматривается способ реализации такого метода на примере устройства [7].

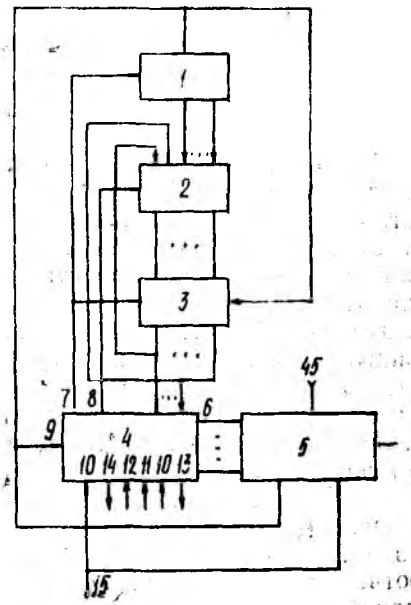

Рис. 1

Формирование имитостойких последовательностей ДЧС (КДЧС). На рис. 1 представлена схема устройства; на рис. 2 — схема мультипликатора; на рис. 3 — схема блока выдачи дискретных частотных сигналов.

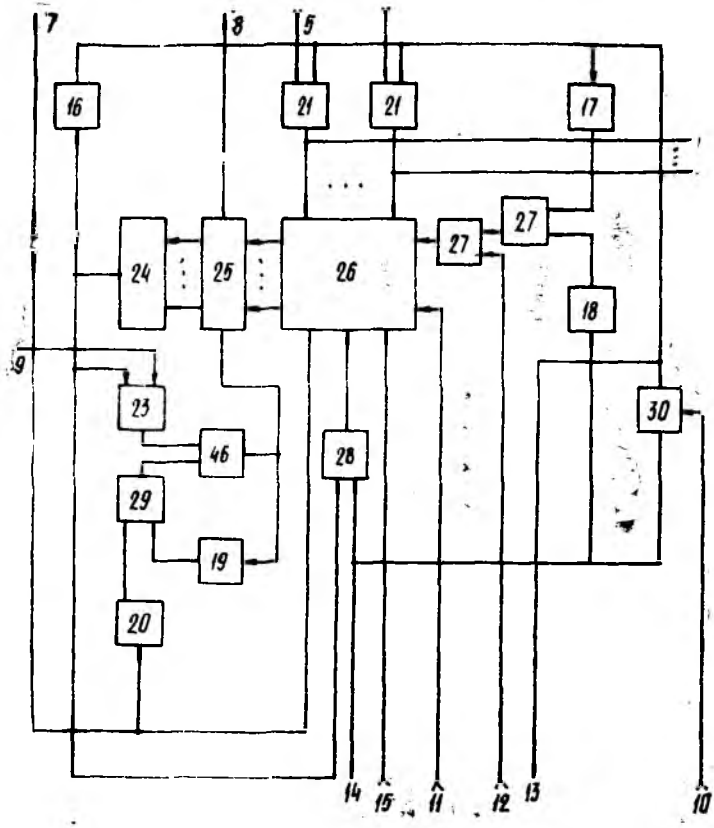

Рис 2.

Устройство содержит счетчик *1*, формирователь остатков *2*, регистр *3*, мультипликатор *4*, блок *5* выдачи дискретных частотных сигналов, входы и выходы *6—15*, элементы задержки *16—20*, группу *21* элементов И, элементы И—НЕ *22—24*, регистр сдвига *25*, блок *26* умножения, элементы ИЛИ *27—29*, счетчик элементов *30*, дешифратор *31*, распределитель импульсов *32*, генератор тактовых импульсов *33*, элементы коммутации *34*, группа генераторов эталонных частот *35*, элемент И *36*, делитель *37*, аналого-цифровой преобразователь (АЦП) *38*, элемент ИЛИ *39*, коммутатор каналов *40*, элемент ИЛИ *41*, элемент коммутации *42*, счетчик *43*, генератор импульсов *44*, группу информационных входов устройства *45* и элемент И *46*.

Устройство работает следующим образом.

Перед началом работы в блок *26* умножения мультипликатора *4* записывается двоичный код числа, первообразного элемента Θ_t соответствующего поля Галуа $GF(p^n)$, а на счетчик *30* мультипликатора *4* и в делитель *37* с переменным коэффициентом деления поступает код числа p^n элементов поля $GF(p^n)$. Подачей им-

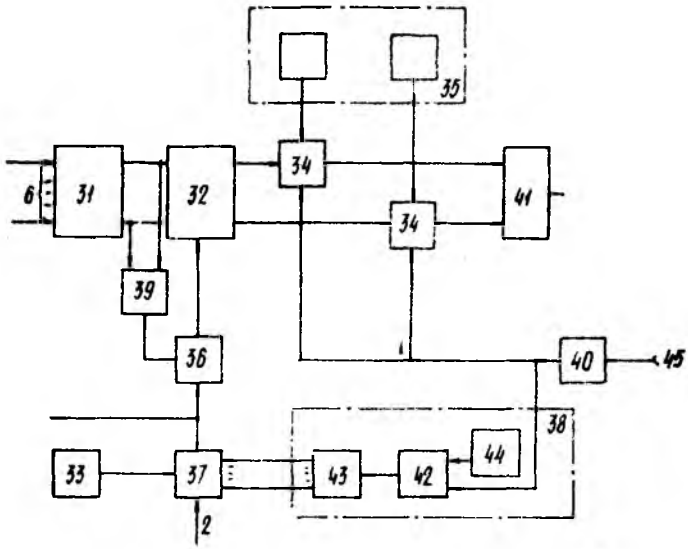

Рис. 3

пульса «Начало работы» устройство включается в работу, на основании этого импульса блок *5* начинает выдавать тактовые импульсы по своему выходу. На основании данных импульсов мультипликатор умножает Θ_i на единицу, а по окончании умножения выдает по своему выходу *7* импульс установки в исходное состояние на счетчик *1* и регистр *3* и затем начинает в каждый тактовый момент выдавать в фомирователь *2* код результата умножения. Формирователь *2* формирует остаток от числа по модулю p_i и выдает результат в регистр *3*. Последний выдает остаток по модулю на входы мультипликатора *4*. Этот остаток результата умножения единицы на Θ_i по модулю p_i и является первым элементом a_1 мультипликативной группы поля Галуа $GF(p_i^n)$. Мультипликатор *4* выдает первый элемент a_1 на входы блока *5* формирования дискретных частотных сигналов. Кроме того, код остатка записывается в блок *26* умножения мультипликатора *4*, где происходит процесс перемножения a_j на Θ_i. Затем повторяется указанный цикл операций и формируется второй элемент a_2 мультипликативной группы поля GF и т. д. Таким образом, на входе мультипликатора *4* появляется последовательность кодов остатков

$$a_1 = \Theta_i \pmod{p_i},\quad a_2 \equiv \Theta_i^2 \pmod{p_i},\quad \ldots,\quad a_j \equiv \Theta_i^j \pmod{p_i}.$$

Эта последовательность параллельных двоичных кодов остатков a_1, a_2, ..., a_j представляет собой последовательность элементов мультипликативной группы поля $GF(p_i^n)$.

Последовательность параллельных двоичных кодов остатков поступает на блок *5*, где происходит образование сложных сигналов в соответствии с информацией модуля p_i, поступающей в блок *5*, и длительностью информационного импульса. По окончании

формирования элементов мультипликативной группы с выхода мультипликатора поступает импульс «Конец формирования мультипликативной группы поля $GF\ (p^n)$», и на основании этого импульса на вход мультипликатора *4* поступают такты прямого считывания. Блок *5*, в котором с приходом последнего элемента мультипликативной группы сформировался сложный сигнал, выдает в соответствии с тактами этот сложный сигнал по своему выходу.

Устройство имеет следующие режимы работы.

Режим 1. При фиксированной длительности информационной посылки: а) с изменением первообразного Θ_i; б) с изменением модуля p_i.

Режим 2. При изменении длительности информационной посылки: а) с изменением первообразного Θ_i; б) с изменением модуля p_i.

Режим 1, а характеризуется изменением частотного и временного положений элементов сигнала на частотно-временной матрице (базового прямоугольника).

Режим 1, б характеризуется изменением количества частотных интервалов на частотно-временной матрице.

Режим 2, а характеризуется изменением частотного и временного положений элементов сигнала, а также длительности сигнала.

Режим 2, б характеризуется изменением количества частотных интервалов и длительности сигнала.

Формирование элементов мультипликативных групп полей Галуа обеспечивает мультипликатор *4*, работающий следующим образом.

Перед началом работы в блок *26* умножения по входам *11* и *15* записывается двоичный код числа первообразного элемента Θ_i соответствующего поля $GF(p^n)$ в регистр множителя и единица в регистр множимого, а также по входу *10* в счетчик *30* записывается код числа элементов поля. Подачей импульса «Начало вычисления» по входу *12* на вход «Начало умножения» блока *26* устройство включается в работу. Блок *26* умножает единицу на Θ_i и записывает результат умножения в регистр *25* сдвига, а по окончании умножения выдает по соответствующему выходу импульс «Конец умножения» на выход, приводя в нулевое состояние счетчик *1* и регистр *3*, и на элемент *20* задержки. В следующий тактовый момент импульсом с выхода элемента *20* через элемент ИЛИ *29* открывается элемент И *46*, позволяя тактовому импульсу с выхода элемента И—НЕ *23* пройти на тактовый вход регистра *25* сдвига на элемент *19* задержки, который обеспечивает открытие элемента И *46* в последующие тактовые моменты и прохождения импульсов на тактовый вход регистра сдвига. Таким образом, считываемое с регистра *25* число $A_1=\Theta_i\cdot 1$ в двоичном коде поступает, начиная с младшего разряда, на вход формирователя *2*. Тактовые импульсы, поступающие на вход *9*, сопровождают импульсы кода, считываемого с регистра *25* числа, и поступают на счетчик. Количество состояний счетчика *1* определяется из рассмотрения остатка от деления веса каждого разряда считываемого числа A_1 на вы-

бранный модуль p_i поля $GF(p_i^n)$. Если получаемая последовательность цифр имеет период повторения, то количество состояний счетчика *1* равно количеству цифр в периоде. Если результат деления представляет некоторую последовательность цифр без периода, то количество состояний счетчика *1* равно количеству разрядов в передаваемом числе. Выходы счетчика *1* соединены с входами формирователя *2* таким образом, что наличие каждого элемента И последнего обусловливается определенным соответствием между состоянием счетчика *1* и последующим разрядом числа. Выходные сигналы формирователя *2* при наличии тактовых импульсов на входе запоминаются в регистре *3*, имеющем количество разрядов, необходимое для представления наименьшего остатка по модулю p_i. При этом каждому триггеру регистра *3* соответствуют два элемента ИЛИ формирователя *2* (для установки в «0» или в «1»), причем каждому элементу ИЛИ последнего соответствует такое число элементов И последнего, сколько возможных ситуаций приводит к переводу триггера в соответствующее состояние. Таким образом, на выходах разрядов регистра *3* в каждый тактовый момент появляется двоичный код остатка по модулю p_i от поступившего к этому моменту на вход формирователя *2* двоичного числа. В момент считывания последнего (высшего) разряда числа на выходах разрядов регистра *3* появляется код остатка по модулю p_i от числа $a_1 = A_1 \pmod{p_i}$. В тот же момент регистр *25* обнуляется, и на выходе элемента И—НЕ *24* появляется импульс «Конец считывания», который поступает на другой вход элемента И—НЕ *23*, прекращая тем самым прохождение тактовых импульсов на тактовый вход регистра *25* и через элемент ИЛИ *28* на соответствующий вход блока *26*, приводя в нулевое состояние его регистр множимого. В следующий момент, пройдя элемент *16* задержки, данный импульс поступает на счетный вход счетчика *30* и на входы элементов И *21*, открывая их и обеспечивая считывание с регистра *3* в параллельном коде остатка a_{i-1} по модулю p_i от числа A_1 на входы записи множимого числа в регистр множимого блока *26* в следующий тактовый момент. Пройдя элемент *17* задержки, данный импульс проходит через элемент И—НЕ *22*, элемент ИЛИ *27* — на вход блока *26*, обеспечивая умножение множимого числа $a_1 = \Theta_1 \pmod{p_i}$ на множитель Θ_i. Результат умножения $A_2 = a_1\Theta_i = \Theta^2 i$ записывается в регистр *25* сдвига.

Затем повторяется цикл операций, описанный для числа A_1, на входах устройства появляется код остатка, который в блоке *26* умножения на Θ_i, и в регистр *25* записывается следующий результат $A_3 = a_2\Theta_i$. Затем цикл операций повторяется и т. д. Таким образом, на выходе устройства появляется последовательность кодов остатков. Процесс формирования данной последовательности кодов остатков продолжается до тех пор, пока счетчик *30* элементов, на счетный вход которого поступают импульсы «Момент считывания a_j», не переполнится и не выдаст импульс переполнения, поступающий на выход и через элемент ИЛИ *28* на соответствующий вход блока *26*, обнуляя его регистр множимого, в котором к этому мо-

менту записан код последнего остатка, а также через элемент *18* задержки на другой вход элемента И—НЕ *22*, запрещая прохождение импульса с выхода элемента *17* задержки на вход блока *26*. При этом устройство подготавливается к новому циклу вычислений.

Таким образом, на выходах *6* формируется последовательность параллельных двоичных кодов остатков, представляющих собой последовательность элементов мультипликативной группы поля Галуа, которые поступают на вход блока *5*.

Блок *5* сигналов работает следующим образом. Остаток в параллельном коде поступает с выходов *6* мультипликатора на входы дешифратора *31*. Дешифратор *31* преобразует двоичный код числа в сигнал только на одном из своих выходов. Этот сигнал (импульс) поступает на управляющий вход распределителя *32* и через элемент ИЛИ *39* на вход элемента И *36*. На вход АЦП *38* с выхода коммутатора *40* поступает последовательность информационных импульсов, уплотненных по времени.

АЦП *38* преобразует длительность информационного импульса в цифровой код. Информационный импульс открывает на время Т элемент *42*, на второй вход которого подаются импульсы от генератора *44* импульсов, с выхода элемента *42* эти импульсы поступают на вход счетчика *43*. Счетчик считает число поступивших импульсов, количество которых зависит от интервала Т.

С выхода счетчика *43* снимается код. Таким образом, АЦП *38* преобразует длительность информационного импульса в цифровой код, который поступает на делитель *37* с переменным коэффициентом деления. На входы делителя *37* подаются импульсы генератора *33* тактовых импульсов и код модуля числа p_i. Делитель *37* в соответствии с поступившими на его входы цифровым кодом с выхода АЦП *38* и кодом модуля числа p_i изменяет коэффициент деления и выдает последовательность импульсов с изменением в соответствии с кодом периода их следования. Последовательность импульсов с выхода делителя *37* подается на первые входы счетчика *1*, регистра *3* и мультипликатора *4* и является для них тактовой последовательностью импульсов. Эти же импульсы проходят через элемент И *36*, открытый сигналом с выхода элемента ИЛИ *39*, на вход распределителя *32* в такой последовательности, которая определяется номером входа распределителя *32*, на котором существует сигнал с дешифратора *31*. С выходов распределителя *32* импульсы поступают на входы элементов *34*, на вторые входы которых подается сигнал с группы *35* генераторов, а на третьи — сигнал с выхода коммутатора *40*.

Каждому информационному импульсу на выходе коммутатора *40* соответствует определенный остаток на входе дешифратора *31*, а следовательно, и определенный порядок распределения импульсов по выходам распределителя *32*. Таким образом, элементы *34* открываются поочередно в порядке, определенном для каждого информационного импульса, пропуская на выход через элемент ИЛИ *41* одну из частот. Очередность открывания элементов *34*

определяет структуру сигнала. Этот порядок определяется первообразным элементом поля Θ_i, модулем p_i и длительностью информационной посылки T. Таким образом, каждой информационной посылке определенного абонентского комплекта соответствует свой определенный сложный сигнал. На выходе блока *5* формируется последовательность дискретных частотных сигналов в соответствии с последовательностью параллельных двоичных кодов остатков a_1, a_2, ..., a_j на выходе образующего мультипликатора, представляющая собой последовательность элементов мультипликативной группы полей Галуа. Работа блока *5* в различных режимах практически одинакова. В режиме 1, а (при фиксированной длительности информационной посылки с изменением первообразного Θ_i) в результате изменения первообразного Θ_i происходит изменение последовательности кодов элементов того же поля на входах дешифратора *31*. Это приводит к тому, что управляющий работой распределителя *32* сигнал (импульс) появляется на другом выходе дешифратора *31*, а это изменяет режим работы распределителя *32*, который распределяет импульсы в другой последовательности, а следовательно, и коммутирует элементы *34* в другой последовательности, что приводит к изменению частотного и временного положений элементов сигнала на частотно-временной матрице. В режиме 1, б (при фиксированной длительности информационной посылки с изменением кода модуля p_i), в результате изменения кода модуля p_i изменяется коэффициент деления делителя *37*, выходные импульсы которого являются тактовыми импульсами. Делитель *37* изменяет частоту этих тактовых импульсов, а следовательно, и распределитель *32* подключает большее или меньшее (в зависимости от значения p_i) количество элементов *34* во время фиксированной длительности информационной посылки T, т. е. происходит изменение количества интервалов на частотно-временной матрице.

В режиме 2, а (при изменении длительности информационной посылки *T* с изменением первообразного Θ_i) в результате изменения длительности информационной посылки T изменяется цифровой код на выходах АЦП *38*, этот код, являющийся управляющим для делителя *37*, изменяет коэффициент деления делителя *37*, а следовательно, частоту следования выходных импульсов делителя *37*, которые являются тактовыми импульсами для мультипликатора *4*, счетчик *1*, регистра *3* и распределителя *32*. Это изменяет фактическое время подключения элементов *34*, а следовательно, фактическое время генерирования частот. В результате изменения первообразного Θ_i происходят процессы, описанные в режиме 1, а. Следовательно, в режиме *2, а* происходит изменение частотного и временного положений элементов сигнала на частотно-временной матрице и длительности сигнала. В режиме *2 б* (при изменении длительности информационной посылки T с изменением модуля p_i) изменяется длительность информационной посылки, а следовательно, код на выходах АЦП *38* и код модуля p_i. Эти коды

являются управляющими для делителя *37*, в результате двойного управления делитель *37* изменяет коэффициент деления — частоту следования своих выходных импульсов, что изменяет фактическое время подключения элементов *34*, а следовательно, фактическое время генерирования частот и изменяет число подключаемых элементов *34*, т. е. количество частотных интервалов. Следовательно, в режиме *2*, б происходит изменение количества частотных интервалов и длительности дискретного частотного сигнала.

Записывая в устройство коды иных первообразных элементов Θ_i, иных чисел элементов p_i, можно сформировать любые другие последовательности сигналов. Изменяя структуру формирования остатков с целью формирования остатков по иному модулю, можно сформировать последовательности сложных сигналов других полей.

Понятно, что для формирования КДЧС можно использовать и другие закономерности, известные в алгебре, подобные конечным полям Галуа в этом смысле. Однако это, во-первых, потребует разработки соответствующих аппаратных средств, формирующих техническими способами такие закономерности, тогда как для формирования конечных полей Галуа такие средства разработаны, а, во-вторых, в алгебраической теории вряд ли можно отыскать закономерности, обладающие такими большими возможностями для формирования КДЧС, какими обладают конечные поля Галуа. Хотя, безусловно, будут найдены и другие оригинальные и эффективные пути решения этой важной задачи.

Список литературы: 1. *Варакин Л. Е.* Теория систем сигналов. М., 1978. 304 с. 2. *Диффи У., Хэлман М.* Защищенность и имитостойкость. Введение в криптографию // Тр. Ин-та инж. 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. М.* Энтропийная оценка скрытности радиопередачи // Радиотехника. М., 1980. № 4. С. 32—36. 6. *Постников М. М.* Теория Галуа. М., 1963. 218 с. 7. *А. с. 1203533 СССР.* Устройство для формирования имитостойких последовательностей сигналов сложной формы / И. И. Снытkин, И. Д. Горбенко // Открытия. Изобретения. 1986. № 1. С. 222.

Поступила в редколлегию 19.10.88

УДК 681.326.7

М. Ю. ЛОСЕВ, канд. техн. наук, *А. Н. РЫСОВАНЫЙ*

СИНТЕЗ ГРУППОВОГО МНОГОКАНАЛЬНОГО СИГНАТУРНОГО АНАЛИЗАТОРА

В настоящее время большое количество работ посвящено вопросам построения, оценке эффективности функционирования и применения сигнатурных анализаторов при контроле и диагностике