В. Г. Стародубцев, Формирование пятеричных последовательностей Гордона–Миллса–Велча для систем передачи дискретной информации, *Тр. СПИИРАН*, 2019, выпуск 18, том 4, 912–948

DOI: 10.15622/sp.2019.18.4.912-948

УДК 519.725; 512.62 **DOI** 10.15622/sp.2019.18.4.912-948

В.Г. СТАРОДУБЦЕВ

ФОРМИРОВАНИЕ ПЯТЕРИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА — МИЛЛСА — ВЕЛЧА ДЛЯ СИСТЕМ ПЕРЕДАЧИ ДИСКРЕТНОЙ ИНФОРМАЦИИ

Стародубцев В.Г. **Формирование пятеричных последовательностей Гордона — Миллса — Велча для систем передачи дискретной информации.**

Аннотация. Предложен алгоритм формирования пятеричных последовательностей Гордона-Миллса-Велча (ГМВ) с периодом N=624 над конечным полем с двойным расширением, основанный на матричном представлении базисной М-последовательности с примитивным проверочным полиномом четвертой степени и аналогичным периодом. Показано, что проверочный полином ГМВ-последовательности может быть представлен в виде произведения нескольких неприводимых над простым полем GF(5) полиномов-сомножителей четвертой степени. Получены соотношения между корнями полинома базисной М-последовательности и корнями полиномов-сомножителей, на основании которых может быть сформирован весь перечень ГМВ-последовательностей с периодом N=624. Показано, что для каждого из 48 примитивных полиномов четвертой степени, являющихся проверочными полиномами для базисных М-последовательностей, может быть сформировано по три ГМВ-последовательности с эквивалентной линейной сложностью (ЭЛС), равной 12, 24 или 40, характеризующей структурную скрытность псевдослучайных последовательностей (ПСП). Представлено устройство формирования ГМВ-последовательности в виде совокупности регистров сдвига с линейными обратными связями, в котором умножители и сумматоры по mod5 расставляются в соответствии с коэффициентами неприводимых полиномов-сомножителей. Начальные состояния ячеек регистров сдвига определяются путем децимации символов базисной М-последовательности по индексам децимации, равным минимальным показателям степени корней полиномов-сомножителей. Особенностью определения начальных состояний устройств формирования пятеричных ГМВ-последовательностей по сравнению с двоичными является наличие циклических сдвигов суммируемых последовательностей на величину, кратную $N/(p-1)$. Полученные результаты позволяют синтезировать устройства формирования полного перечня из 144 пятеричных ГМВ-последовательностей с периодом N=624 и различной ЭЛС. Применение ГМВ-последовательностей по сравнению с М-последовательностями позволяет существенно (в 3 – 10 раз) повысить структурную скрытность передаваемых широкополосных сигналов в системах передачи дискретной информации. Результаты исследований могут быть использованы при построении других классов псевдослучайных последовательностей, допускающих аналитическое представление в конечных полях.

Ключевые слова: псевдослучайные последовательности, конечные поля, неприводимые, примитивные и минимальные полиномы, эквивалентная линейная сложность, децимация, регистры сдвига.

1. Введение. В современных системах передачи дискретной информации, включающих системы управления, связи и навигации, широкое применение получили сигналы с расширенным спектром (СРС), которые строятся на основе дискретных ПСП с заданными корреляционными и структурными свойствами [1-2]. В данных работах проведен анализ применения ПСП в системах связи с множественным доступом с кодовым разделением в основном для двоичных последовательностей.

Также ПСП могут быть использованы в системах передачи информации в качестве синхронизирующих, скремблирующих последовательностей, в виде последовательностей, расширяющих спектр передаваемых сигналов для широкополосных радиоканалов, а также для формирования систем сигналов сложной формы с хорошими периодическими автокорреляционными (ПАКФ) и взаимно корреляционными функциями (ПВКФ) [3-4]. При этом в [3] подробно рассмотрены вопросы формирования и применения двоичных ПСП с двухуровневой ПАКФ, например М-последовательностей. В [4] наряду с анализом применения двоичных последовательностей в системах связи с множественным доступом рассматриваются и вопросы формирования троичных последовательностей.

В системах передачи данных по радиоканалам при выборе ПСП должны учитываться как их корреляционные функции, так и структурная скрытность. В качестве показателя структурной скрытности ПСП используется такой параметр, как ЭЛС, численно равный степени проверочного полинома, на основании которого формируется данная последовательность [5-6]. В данных работах приведены оценки для ЭЛС двоичных последовательностей, которые определяются через параметры конечных групп и полей.

В существующих телекоммуникационных системах применяются в основном двоичные М-последовательности, последовательности Голда, малого и большого множеств Касами, а также ГМВ-последовательности [7-10]. В [7] наряду с двоичными ПСП проведен анализ корреляционных и структурных свойств троичных последовательностей над полями нечетных характеристик и характеристики «два», а также составных троичных последовательностей. В работах [8-9] рассмотрены вопросы формирования и оценки структурных свойств двоичных ГМВ-последовательностей. В [10] показана аппаратная и программная реализация алгоритма формирования ГМВ-последовательностей. В [11] приведен алгоритм синтеза фазоманипулированных сигналов с высокой структурной скрытностью.

Вопросам разработки алгоритмов и устройств формирования недвоичных ПСП посвящено большое количество работ как в нашей стране, так и за рубежом [12-14]. В [12] рассмотрены вопросы применения недвоичных последовательностей с точки зрения контроля функционирования устройств декодирования помехоустойчивых кодов. В [13] разработан алгоритм формирования и выполнена оценка линейной сложности троичных ГМВ-последовательностей с периодом N=80. В [14] представлено семейство p-ичных последовательностей с небольшими значениями корреляционной функции. В [15-16] проведен достаточно подробный анализ состояния вопроса формирования

недвоичных ПСП и систем ПСП с заданными корреляционными и структурными свойствами. В работах [15, 17] формирование недвоичных последовательностей осуществляется путем децимации М-последовательностей. В [18] проведен анализ взаимно корреляционных свойств М-последовательностей. В [19] рассмотрены вопросы формирования широкополосных сигналов на основе прямого расширения спектра троичной М-последовательностью. В работах [20-23] приведены результаты по формированию семейств недвоичных последовательностей с низкими уровнями взаимно корреляционных функций. Рассматриваются вопросы синтеза как троичных, так и p-ичных ПСП.

Проведенный анализ показывает, что перспективным направлением развития систем передачи данных является переход от двоичных к многопозиционным сигналам. Недвоичные сигналы с расширенным спектром формируются на основе недвоичных ПСП и обладают более высокой информативностью и структурной скрытностью.

Среди недвоичных последовательностей, обладающих одинаковой двухуровневой ПАКФ, можно выделить М-последовательности и ГМВ-последовательности. При этом предпочтительность применения ГМВ-последовательностей определяется их более высокой структурной скрытностью по сравнению с М-последовательностями.

Широкому применению недвоичных ГМВ-последовательностей в системах передачи данных препятствует отсутствие практически реализуемых алгоритмов формирования данных последовательностей.

Цель исследования — разработка алгоритма формирования пятеричных ГМВ-последовательностей с периодом N=624, основанного на матричном представлении базисной М-последовательности с использованием структурных свойств проверочных полиномов.

2. Последовательности Гордона — Миллса — Велча над GF(p). Формирование ГМВ-последовательностей осуществляется в конечных полях с двойным расширением $\mathrm{GF}[(p^m)^n]=\mathrm{GF}(p^S)$ ($S=m\cdot n$). Период последовательностей является составным числом, то есть $N=p^{mn}-1$.

Символы d_i ГМВ-последовательности с периодом $N=p^{mn}-1$ определяются выражением [8, 9]:

$$d_i=\mathrm{tr}_{m1}[(\mathrm{tr}_{mn,m}(\alpha^i))^r],\ \ 1\le r<p^m-1,\ \ (r,p^m-1)=1, \qquad (1)$$

где $\mathrm{tr}_{mn,m}(\cdot)$ — след элемента, принадлежащего полю $\mathrm{GF}[(p^m)^n]$, в расширенном поле $\mathrm{GF}(p^m)$; $\mathrm{tr}_{m1}(\cdot)$ — след элемента поля $\mathrm{GF}(p^m)$ в простом поле $\mathrm{GF}(p)$; $\alpha\in\mathrm{GF}[(p^m)^n]$ — примитивный элемент; r — натуральное число, взаимно простое с порядком мультипликативной группы поля $\mathrm{GF}(p^m)$, равным p^m-1.

Структурная скрытность ПСП определяется ЭЛС, которая для двоичных ГМВ-последовательностей определяется выражением [5, 8]:

$$l_S = m \cdot n^{g(r)}, \tag{2}$$

где $g(r)$ — количество единиц в двоичном представлении числа r в (1).

Количество различных ГМВ-последовательностей определяется как произведение числа примитивных полиномов в подполе $GF(p^m)$ на число примитивных полиномов в поле $GF[(p^m)^n]$ [9]:

$$M_\Gamma = (\frac{\varphi(p^m - 1)}{m} - 1) \cdot \frac{\varphi(p^{mn} - 1)}{mn}, \tag{3}$$

где $\varphi(a)$ — функция Эйлера, равная числу чисел, взаимно простых с числом a, в ряду от 1 до $(a - 1)$.

Формирование ГМВ-последовательности осуществляется на основе М-последовательности с аналогичным периодом, построение которой реализуется с помощью примитивного полинома, называемого проверочным и определяемого из таблиц неприводимых полиномов [24].

В [5, 9-10] показано, что двоичные ГМВ-последовательности строятся над конечными полями с двойным расширением вида $GF[(2^m)^n]$ путем представления М-последовательностей, которые будем называть базисными последовательностями, в виде матрицы размерности $[J \times L]=[(2^m-1)\times(2^m+1)]$.

Для формирования недвоичных ГМВ-последовательностей может быть использован аналогичный подход с учетом особенностей построения конечных полей с характеристикой $p > 2$.

При вычислении периодических корреляционных функций наблюдается ряд особенностей, связанных с представлением символов d_i недвоичных последовательностей в виде элементов комплекснозначного алфавита, то есть корней p-й степени из единицы или элементов простого поля $GF(p)$.

Форма представления символов d_i определяет вид пространства, в котором вычисляется корреляционная функция, и способ определения расстояния между последовательностями, то есть метрику пространства.

Если символы d_i принадлежат комплекснозначному алфавиту, то при вычислении корреляционных функций используется метрика в Евклидовом пространстве [2, 3].

Если символы d_i принадлежат простому полю $GF(p)$, то используется метрика Ли при $p > 2$. При этом расстояния между элементами d_i и d_j в метрике Ли определяется выражением:

$$q_{\text{ЛИ}}(d_i, d_j) = \begin{cases} |d_i - d_j|, & \text{если } |d_i - d_j| \le p/2, \\ p - |d_i - d_j|, & \text{если } |d_i - d_j| > p/2. \end{cases} \quad (4)$$

Можно дать следующую интерпретацию расстояния Ли между двумя элементами. Если p элементов равномерно расположить на окружности в порядке возрастания их номеров от 0 до p–1, то расстояние Ли определяется числом участков окружности при движении от одного элемента к другому по кратчайшей дуге.

С учетом метрики Ли вида (4) расстояние между недвоичными последовательностями A_j и A_k для различных циклических сдвигов λ определяется выражением:

$$D_{jk}(\lambda) = \sum_{l=0}^{N-1} q(d_{jl}, d_{k,l+\lambda}). \quad (5)$$

Максимальному значению периодической корреляционной функции $R_{\max} = N$ соответствует минимальное расстояние $D_{\min} = 0$ при совпадении всех элементов последовательностей. Минимальному значению периодической корреляционной функции $R_{\min} = -N$ соответствует максимальное значение расстояния $D_{\max} = pN/2$, достигаемое в случае, когда соответствующие элементы последовательностей противоположны.

На рисунке 1 показано совмещение шкал D и R, которые являются разнонаправленными.

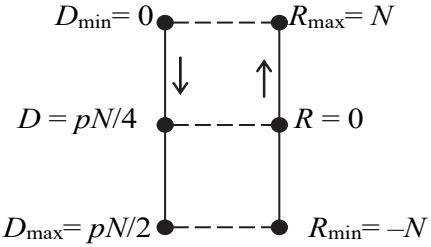

Рис.1. Совмещение шкал расстояния D и корреляции R

С учетом линейности операции преобразования шкал можно получить выражение для корреляционной функции p-ичных последовательностей в общем случае через расстояние D в метрике Ли:

$$R_{jk}(\lambda) = N - \frac{4}{p} D_{jk}(\lambda). \quad (6)$$

При использовании метрики Ли максимальное значение расстояния $D_{\max} = pN/2$ достигается только при наличии противоположных элементов, то есть при четном p. При нечетном p максимальное расстояние $D_{\max} = N(p–1)/2$.

ГМВ-последовательности и М-последовательности представляют собой p-ичные ПСП с периодом $N = p^S–1$, построенные над полем GF(p^S) и имеющие в метрике Евклида двухуровневую ненормированную ПАКФ:

$$R(\lambda) = \begin{cases} N & \text{при } \lambda = kN, k = 0,1,2,..., \\ -1 & \text{при } \lambda \neq kN. \end{cases} \quad (7)$$

Выражение (7) справедливо в метрике Евклида как для двоичных, так и для p-ичных ПСП. В метрике Ли для p-ичных ПСП ПАКФ также является двухуровневой, при этом значение второго уровня зависит от периода N и величины p.

Пояснить это можно следующим образом. При вычислении ПАКФ М-последовательности и ГМВ-последовательности число различных попарных сочетаний символов равно p^2. Например, для p=5, имеется p^2=25 возможных попарных сочетаний символов: 0-0, 0-1, …, 0-4, 1-0, 1-1, …, 4-3, 4-4. При этом число каждого попарного сочетания символов в последовательностях для произвольного сдвига λ зависит от периода N и одинаково для всех сочетаний, кроме сочетания 0-0, число которых на единицу меньше.

Например, для пятеричных М-последовательностей и ГМВ-последовательностей с периодом N=624 над конечным полем с двойным расширением GF[$(5^2)^2$] каждое сочетание встречается ровно 25 раз, а сочетание 0-0 встречается 24 раза. В соответствии с (4) расстояние между пятеричными символами может принимать только три значения: 0, 1 и 2. При вычислении расстояния D учитываются 250 сочетаний с расстоянием $d_{ЛИ}$=1 и 250 сочетаний с расстоянием $d_{ЛИ}$=2 (124 сочетания одинаковых символов не изменяют расстояния). В результате D=750, а значение ПАКФ, в соответствии с (6), равно $R_{jj}(\lambda)$= 24.

В общем случае для p-ичных М-последовательностей и ГМВ-последовательностей с периодом $N=p^S$-1 двухуровневая ненормированная ПАКФ в метрике Ли в отличии от (7) зависит от основания p и имеет вид:

$$R(\lambda) = \begin{cases} N & \text{при } \lambda = kN, k = 0,1,2,..., \\ p^{S-2} - 1 & \text{при } \lambda \neq kN. \end{cases} \quad (8)$$

Достоинством определения корреляционных функций p-ичных М-последовательностей и ГМВ-последовательностей в метрике Ли является то, что все вычисления осуществляются в области целых чисел по mod p.

3. Формирование ГМВ-последовательностей с периодом N=24. Разработку алгоритма формирования пятеричных ГМВ-последовательностей проведем на последовательности с периодом $N = 5^2–1=24$.

В этом случае формирование ГМВ-последовательностей осуществляется в расширенном поле $GF[(p^m)^n]=GF[(5^1)^2]=GF(5^2)$. Период последовательностей является составным числом, то есть $N = p^{mn}–1$.

Примитивный полином $f(x)=x^S+f_{S-1}x^{S-1}+\ldots+f_2x^2+f_1x+f_0$ с корнем α^1, в соответствии с которым строится поле и относительно которого формируются все другие неприводимые полиномы степени S и делителей S в конечном поле $GF(p^S)$, где S — степень расширения поля, может быть выбран произвольно, но обычно принято в качестве исходного полинома использовать примитивный полином с наименьшим числом слагаемых и минимальными коэффициентами при переменной x. В поле $GF(5^2)$ таким полиномом является примитивный полином $f(x)=x^2+x+2$.

Таким образом, построение поля $GF(5^2)$ выполним по примитивному полиному $f(x)=x^2+x+2$, одним из корней которого является примитивный элемент $\alpha = a$ (таблица 1).

Таблица 1. Элементы расширенного поля $GF(5^2)$, $f(x)=x^2+x+2$, $\alpha = a$

Формы элементов поля			Минимальный полином	Период	Корни	След $tr_{2,1}\,\alpha$
Степенная	Полиномиальная	Векторная				
$\alpha^{-\infty}$	0	00	$h_{-\infty}(x) = x$	1	0	0
α^0	1	01	$h_0(x)= x–1 = x+4$	1	α^0	2
α^1	a	10	$h_1(x) = x^2+x+2$	24	α^1, α^5	4
α^2	$4a+3$	43	$h_2(x) = x^2+3x+4$	12	α^2, α^{10}	2
α^3	$4a+2$	42	$h_3(x) = x^2+3$	8	α^3, α^{15}	0
α^4	$3a+2$	32	$h_4(x) = x^2+4x+1$	6	α^4, α^{20}	1
α^5	$4a+4$	44	$h_1(x) = x^2+x+2$	24	α^5, α^1	4
α^6	2	02	$h_6(x) = x+3$	4	α^6	4
α^7	$2a$	20	$h_7(x) = x^2+2x+3$	24	α^7, α^{11}	3
α^8	$3a+1$	31	$h_8(x) = x^2+x+1$	3	α^8, α^{16}	4
α^9	$3a+4$	34	$h_9(x) = x^2+2$	8	α^9, α^{21}	0
α^{10}	$a+4$	14	$h_2(x) = x^2+3x+4$	12	α^{10}, α^2	2
α^{11}	$3a+3$	33	$h_7(x) = x^2+2x+3$	24	α^{11}, α^7	3
α^{12}	4	04	$h_{12}(x) = x+1$	2	α^{12}	3
α^{13}	$4a$	40	$h_{13}(x) = x^2+4x+2$	24	α^{13}, α^{17}	1
α^{14}	$a+2$	12	$h_{14}(x) = x^2+2x+4$	12	α^{14}, α^{22}	3
α^{15}	$a+3$	13	$h_3(x) = x^2+3$	8	α^{15}, α^3	0

Труды СПИИРАН. 2019. Том 18 № 4. ISSN 2078-9181 (печ.),
ISSN 2078-9599 (онлайн), www.proceedings.spiiras.nw.ru

Продолжение таблицы 1

Формы элементов поля			Минимальный полином	Период	Корни	След $tr_{2,1}\ \alpha$
Степенная	Полиномиальная	Векторная				
α^{16}	$2a+3$	23	$h_8(x) = x^2+x+1$	3	α^{16}, α^{8}	4
α^{17}	$a+1$	11	$h_{13}(x) = x^2+4x+2$	24	α^{17}, α^{13}	1
α^{18}	3	03	$h_{18}(x) = x+2$	4	α^{18}	1
α^{19}	$3a$	30	$h_{19}(x) = x^2+3x+3$	24	α^{19}, α^{23}	2
α^{20}	$2a+4$	24	$h_4(x) = x^2+4x+1$	6	α^{20}, α^{4}	1
α^{21}	$2a+1$	21	$h_9(x) = x^2+2$	8	α^{21}, α^{9}	0
α^{22}	$4a+1$	41	$h_{14}(x) = x^2+2x+4$	12	α^{22}, α^{14}	3
α^{23}	$2a+2$	22	$h_{19}(x) = x^2+3x+3$	24	α^{23}, α^{19}	2

Элементы, минимальные полиномы и функции следа элементов данного поля также будут использованы при формировании ГМВ-последовательностей с периодом $N = 5^4–1 = 624$ в поле GF(5^4). Особенно интересен случай, когда коэффициент f_1 при x^1 в примитивном полиноме $f(x)$ равен 1, что позволяет определять начало М-последовательности, формируемой на основе данного примитивного полинома, в соответствии с методикой, которая была разработана в [9, 13], без построения основного поля.

Так как коэффициент f_1 равен значению функции следа $tr_{2,1}\alpha^1$, взятому со знаком «минус», то след элемента α^1 равен $tr_{2,1}\alpha^1 = p–1$. Тогда арифметическая сумма функций следа всех p-сопряженных элементов равна $S(p–1)$ и может быть использована для определения начала М-последовательности в соответствии с (1) при значении параметра r=1.

Для обозначения минимальных полиномов для элементов поля GF(p^S) используется обозначение $h_i(x)$, так как данные полиномы являются проверочными полиномами при построении ПСП. Подстрочный индекс i соответствует минимальному показателю степени корней данного полинома. Если минимальный полином является примитивным, то формируемая ПСП является М-последовательностью.

Простое поле GF(5) можно представить как подполе расширенного поля GF(5^2) (таблица 2).

Таблица 2. Элементы простого поля GF(5), $\beta = \alpha^6 = 2$

Формы элементов поля			Минимальный полином	Период	Корни	След $tr_{2,1}\ \alpha^i$
Степенная	Полиномиальная	Векторная				
$\beta^{-\infty} = \alpha^{-\infty}$	0	00	$h_{-\infty}(x) = x$	1	0	0
$\beta^0 = \alpha^0$	1	01	$h_0(x) = x–1 = x+4$	1	α^0	2
$\beta^1 = \alpha^6$	2	02	$h_1(x) = x+3$	4	α^6	4
$\beta^2 = \alpha^{12}$	4	04	$h_2(x) = x+1$	2	α^{12}	3
$\beta^3 = \alpha^{18}$	3	03	$h_3(x) = x+2$	4	α^{18}	1

В поле GF(5) два примитивных элемента $\beta = 2$ и $\beta^3 = 3$ с периодом $E = 4$. В таблице 2 поле построено по примитивному элементу $\beta = \alpha^6 = 2$.

Аналогично можно построить поле по примитивному элементу $\beta = \alpha^{18} = 3$ (таблица 3).

Таблица 3. Элементы простого поля GF(5), $\beta = \alpha^{18} = 3$

Формы элементов поля			Минимальный полином	Период	Корни	След $\mathrm{tr}_{2,1}\,\alpha^i$
Степенная	Полиномиальная	Векторная				
$\beta^{-\infty} = \alpha^{-\infty}$	0	00	$h_{-\infty}(x) = x$	1	0	0
$\beta^0 = \alpha^0$	1	01	$h_0(x) = x-1 = x+4$	1	α^0	2
$\beta^1 = \alpha^{18}$	3	03	$h_1(x) = x+2$	4	α^{18}	1
$\beta^2 = \alpha^{12}$	4	04	$h_2(x) = x+1$	2	α^{12}	3
$\beta^3 = \alpha^6$	2	02	$h_3(x) = x+3$	4	α^6	4

Алгоритм формирования p-ичных ГМВ-последовательностей может быть реализован путем модернизации алгоритма формирования двоичных и троичных ГМВП, разработанного в [9, 13].

Формализованная запись алгоритма.

Шаг 1. Ввод исходных данных:

– выбор минимального примитивного полинома $h_1(x)$ в конечном поле $\mathrm{GF}[(p^m)^n]=\mathrm{GF}(p^S)$;

– задание периода М-последовательности $N = p^{mn} - 1 = p^S - 1$ с параметром $r_1=1$;

– задание параметра ri > r1 , определяющего ЭЛС формируемой ГМВ-последовательности.

Шаг 2. Формирование М-последовательности в соответствии с коэффициентами полинома $h_1(x)$ для S начальных символов $d_0 = \mathrm{tr}_{S,1}\alpha^0$, $d_1 = \mathrm{tr}_{S,1}\alpha^1$, $d_2 = \mathrm{tr}_{S,1}\alpha^2$, …, $d_{S-1} = \mathrm{tr}_{S,1}\alpha^{S-1}$.

Шаг 3. Представление М-последовательности в виде квазиквадратной матрицы $\boldsymbol{F}_{\text{мп}}$ размерности $[J \times L] = [(p^m-1) \times (p^m+1)]$. Столбцы матрицы $\boldsymbol{F}_{\text{мп}}$ (кроме столбца, состоящего из нулей) являются различными циклическими сдвигами более короткой М-последовательности с периодом $N = p^m - 1$, называемой характеристической последовательностью (ХП).

Шаг 4. Определение номеров сдвигов ХП_1, последовательная запись которых образует правило формирования (ПФ) I_p.

Шаг 5. Для последовательности ХП_1 определение по алгоритму Берлекемпа — Месси проверочного полинома $h_{\text{хп1}}(x)$.

Шаг 6. Выбор в таблице неприводимых полиномов поля $\mathrm{GF}(p^m)$ отличного от $h_{\text{хп1}}(x)$ примитивного полинома $h_{\text{хп2}}(x)$ с заданным значением параметра r и формирование различных циклических сдвигов ХП_2.

Шаг 7. Формирование ГМВ-последовательности из базисной М-последовательности путем замены в матрице $\boldsymbol{F}_{\text{мп}}$ столбцов ХП_1 на ХП_2 в соответствии с правилом формирования I_p.

Шаг 8. Определение (по алгоритму Берлекемпа — Месси) проверочного полинома ГМВ-последовательности $h_{\text{г}}(x)$.

Шаг 9. Разложение полинома $h_{\text{г}}(x)$ ГМВ-последовательности и определение полиномов-сомножителей $h_{\text{с}i}(x)$ и минимальных показателей степени их корней, последовательность которых образует вектор сомножителей.

Шаг 10. Построение регистров сдвига с линейными обратными связями (РС ЛОС) в соответствии с полиномами $h_{\text{с}i}(x)$.

Шаг 11. Определение начальных состояний регистров сдвига путем децимации символов базисной М-последовательности в соответствии с показателями степени корней полиномов $h_{\text{с}i}(x)$ и вычисление начальных сдвигов формируемых последовательностей в соответствии с разработанным в [13] алгоритмом.

Шаг 12. Формирование выходной ГМВ-последовательности путем посимвольного сложения последовательностей с выходов регистров сдвига. Конец алгоритма.

Выполним формирование ГМВ-последовательности с периодом $N = p^{mn} - 1 = 5^2\text{-}1=24$ в соответствии с алгоритмом.

Шаг 1. Ввод исходных данных:

– минимальный примитивный полином в конечном поле $\text{GF}[(5^1)^2]=\text{GF}(5^2)$ для формирования базисной М-последовательности: $h_{\text{мп}}(x) = h_1(x) = x^2+x+2$;

– период М-последовательности $N = 24$, параметр $r_1 = 1$;

– задание параметра $r_2 = 2$, определяющего ЭЛС формируемой ГМВ-последовательности.

Шаги 2, 3. Формируемая М-последовательность $\boldsymbol{F}_{\text{мп}}$ в соответствии с (1) при $r_1= 1$ представляет собой последовательность значений функций следа элементов поля (таблица 1), начиная с элемента α^0. Символы М-последовательности $d_0= 2$, $d_1= 4$, $d_2= 2$, $d_3= 0$, $d_4= 1$ и так далее, удовлетворяющие выражению $d_{2+i} = 3d_{0+i} + 4d_{1+i}$ (i=0, 1, …, 21), записываются в виде матрицы размерности $[J\times L] = [4\times 6]$:

$$F_{\text{мп}} = \begin{vmatrix} 2 & 4 & 2 & 0 & 1 & 4 \\ 4 & 3 & 4 & 0 & 2 & 3 \\ 3 & 1 & 3 & 0 & 4 & 1 \\ 1 & 2 & 1 & 0 & 3 & 2 \end{vmatrix}. \qquad (9)$$

Шаг 4. Столбцы матрицы представляют собой различные сдвиги пятеричной М-последовательности с периодом N=4, являющейся

характеристической последовательностью. В качестве нулевого сдвига $ХП_1$ выберем сдвиг 1 2 4 3 из таблицы 2. Последовательность номеров сдвигов образует правило формирования (ПФ) I_p:

$$I_p = (3,\ 2,\ 3,\ –,\ 0,\ 2). \tag{10}$$

Шаг 5. Для последовательности $ХП_1$ проверочный полином определяется по алгоритму Берлекемпа — Месси $h_{хп1}(x) = h_1(x) = x+3$ (таблица 2).

Шаг 6. Выбор в таблице неприводимых полиномов (таблице 2) поля GF(5), $\beta = \alpha^6 = 2$ другого примитивного полинома $h_{хп2}(x) = h_3(x) = x+2$ и формирование различных циклических сдвигов $ХП_2$.

Шаг 7. Формирование ГМВ-последовательности путем замены в матрице $\boldsymbol{F}_{\text{мп}}$ столбцов $ХП_1$ на циклические сдвиги $ХП_2$ в соответствии с правилом формирования $\boldsymbol{I_p}$ вида (10). В качестве нулевого сдвига берется сдвиг «1 3 4 2» из таблицы 3. Тогда матрица (9) преобразуется к виду:

$$I_p = (3 \quad 2 \quad 3 \quad – \quad 0 \quad 2),$$

$$F_{\text{г}} = \begin{vmatrix} 3 & 4 & 3 & 0 & 1 & 4 \\ 4 & 2 & 4 & 0 & 3 & 2 \\ 2 & 1 & 2 & 0 & 4 & 1 \\ 1 & 3 & 1 & 0 & 2 & 3 \end{vmatrix}. \tag{11}$$

Для удобства определения сдвигов $ХП_2$ над матрицей $\boldsymbol{F}_{\text{г}}$ в (11) также приведено полученное ПФ (10).

Шаг 8. Последовательности $\boldsymbol{F}_{\text{мп}}$ и $\boldsymbol{F}_{\text{г}}$ отличаются тем, что произошла замена элементов 2 на 3 и наоборот. Проверочный полином $h_{\text{г}}(x)$ ГМВ-последовательности определяется по алгоритму Берлекемпа — Месси:

$$h_{г}(x) = x^4 + 2x^3 + x^2 + x + 4. \tag{12}$$

Шаг 9. Разложение $h_{\text{г}}(x)$ на неприводимые полиномы в поле $GF(5^2)$ имеет следующий вид:

$$h_{г}(x) = h_{c1}(x)\,h_{c2}(x) = h_3(x)\,h_7(x) = \left(x^2 + 3\right)\left(x^2 + 2x + 3\right). \tag{13}$$

Так как степень полинома в (12) и (13) равна четырем, то ЭЛС ГМВ-последовательности увеличилась в два раза по сравнению с М-последовательностью.

Полином $h_{c1}(x)= h_3(x) = x^2+3$ (таблица 1) является непримитивным, период его корней α^3и α^{15} равен 8. Полином $h_{c2}(x) = h_7(x) = x^2+2x+3$ является примитивным, период его корней α^7 и α^{11} равен 24.

Корни двух полиномов-сомножителей являются 3-ми и 7-ми степенями корней полинома базисной М-последовательности. Данное положение справедливо для произвольной базисной М-последовательности с примитивным полиномом из таблицы 1.

Последовательность минимальных показателей степени корней полиномов-сомножителей $h_{ci}(x)$ образует вектор сомножителей:

$$A=(3,\ 7).$$

Шаг 10. Формирование ГМВ-последовательности реализуется суммированием последовательностей с выходов двух регистров сдвига с проверочными полиномами $h_3(x)$ и $h_7(x)$.

Символы на выходах РС ЛОС определяются коэффициентами полиномов $h_3(x)$ и $h_7(x)$ с помощью рекуррентных выражений:

$$c_{2+i}=2c_{0+i},(i=0,\ 1,\ldots,\ 21), \tag{14}$$

$$c_{2+i}=2c_{0+i}+3c_{1+i},(i=0,\ 1,\ldots,\ 21). \tag{15}$$

Шаг 11. Начальные состояния регистров сдвига определяются путем децимации символов базисной М-последовательности (9) по индексам децимации $i_{d1} = 3$ и $i_{d2} = 7$ и вычисления начальных сдвигов суммируемых последовательностей.

Реализация данного пункта осуществляется по алгоритму, разработанному в [13], поэтому приведем конечные результаты, которые будут получены ниже.

Начальные состояния РС ЛОС: $(d_0, d_3) = (2,3)$ и $(d_{18}, d_1) = (1,4)$.

Шаг 12. ГМВ-последовательность формируется путем посимвольного сложения последовательностей с выходов регистров сдвига с данными начальными состояниями. Отметим, что на периоде ГМВ-последовательности формируется три периода ПСП в регистре с полиномом $h_3(x)$.

На этом выполнение алгоритма заканчивается.

Для двоичных ГМВ-последовательностей значения начальных состояний РС ЛОС определяются путем децимации символов базисной М-последовательности по полученным индексам децимации. При формировании недвоичных ГМВ-последовательностей суммируемые

последовательности с выходов регистров могут иметь определенный циклический сдвиг. Данный сдвиг может принимать значения, кратные величине $N/(p–1)$.

Для определения начальных сдвигов ПСП необходимо в первую очередь найти значения начальных состояний РС ЛОС путем решения системы линейных уравнений при заданном сегменте пятеричной ГМВ-последовательности из (11) длиной 4 символа, например, $d_0 = 3$, $d_1 = 4$, $d_2 = 3$ $d_3 = 0$. Затем определить сдвиги ПСП из условия совпадения начальных состояний регистров.

Для этого составим систему из 4 линейных уравнений вида $x_{ij} + x_{kl} = d_m$, ($i,k = 0, 1$ — номер регистра сдвига; $j,l = 0, 1$ — номер ячейки в регистре; $m = 0, 1, 2, 3$ — номер символа ГМВ-последовательности), каждое из которых определяется с помощью (14)-(15):

$$\begin{aligned} x_{00} + x_{10} &= 3, \\ x_{01} + x_{11} &= 4, \\ 2x_{00} + 2x_{10} + 3x_{11} &= 3, \\ 2x_{01} + x_{10} + x_{11} &= 0. \end{aligned} \tag{16}$$

В результате решения данной системы, например методом последовательного исключения неизвестных, можно получить следующие значения начальных состояний для регистров сдвига:

$$x_{00} = 2;\ \ x_{01} = 0;\ \ x_{10} = 1;\ \ x_{11} = 4.$$

Можно показать, что при таких начальных состояниях двух регистров сдвига на выходе устройства будет формироваться пятеричная ГМВ-последовательность.

В соответствии с алгоритмом определения начальных состояний регистров сдвига [9, 13] значения состояний определяются путем децимации символов базисной М-последовательности по индексам децимации, соответствующим показателям степени корней полиномов-сомножителей. В рассматриваемом примере децимация производится по индексам $i_{d1} = 3$ и $i_{d2} = 7$. В таблице 4 показаны символы d_i базисной М-последовательности F_1 и полученные путем ее децимации символы ПСП F_3 с проверочным полиномом $h_3(x) = x^2+3$ и М-последовательности F_7 с проверочным полиномом $h_7(x) = x^2+2x+3$.

Таблица 4. Определение сдвигов последовательностей F_3 и F_7

	Символы базисной МП с $h_1(x)$, ПСП с $h_3(x)$ и МП с $h_7(x)$																							
h_1: d_i	d_0	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8	d_9	d_{10}	d_{11}	d_{12}	d_{13}	d_{14}	d_{15}	d_{16}	d_{17}	d_{18}	d_{19}	d_{20}	d_{21}	d_{22}	d_{23}
F_1	2	4	2	0	1	4	4	3	4	0	2	3	3	1	3	0	4	1	1	2	1	0	3	2
h_3: d_i	d_0	d_3	d_6	d_9	d_{12}	d_{15}	d_{18}	d_{21}	d_0	d_3	d_6	d_9	d_{12}	d_{15}	d_{18}	d_{21}	d_0	d_3	d_6	d_9	d_{12}	d_{15}	d_{18}	d_{21}
F_3	**2**	**0**	4	0	3	0	1	0	2	0	4	0	3	0	1	0	2	0	4	0	3	0	1	0
h_7: d_i	d_0	d_7	d_{14}	d_{21}	d_4	d_{11}	d_{18}	d_1	d_8	d_{15}	d_{22}	d_5	d_{12}	d_{19}	d_2	d_9	d_{16}	d_{23}	d_6	d_{13}	d_{20}	d_3	d_{10}	d_{17}
F_7	2	3	3	0	1	3	**1**	**4**	4	0	3	4	3	2	2	0	4	2	4	1	1	0	2	1

Шаг 8. Анализ последовательностей F_3 и F_7 показал, что для совмещения начальных состояний регистров и получения ГМВ-последовательности необходимо выполнить сдвиг F_7 относительно F_3 на 0,75 периода вправо, то есть на $3N/(p\text{-}1) = 3*24/4 = 18$ символов. В таблице 5 сформированы последовательности F_3 и F_7 для начальных состояний $(d_0, d_3) = (2,3)$ и $(d_{18}, d_1) = (1,4)$.

Шаг 9. В результате сложения последовательностей F_3 и F_7 по mod5 получается последовательность, совпадающая с матричным представлением ГМВ-последовательности $F_г$ вида (11).

Таблица 5. Формирование ГМВ-последовательности

	Символы базисной МП с $h_1(x)$, ПСП с $h_3(x)$ и МП с $h_7(x)$																							
h_3: d_i	d_0	d_3	d_6	d_9	d_{12}	d_{15}	d_{18}	d_{21}	d_0	d_3	d_6	d_9	d_{12}	d_{15}	d_{18}	d_{21}	d_0	d_3	d_6	d_9	d_{12}	d_{15}	d_{18}	d_0
F_3	**2**	**0**	4	0	3	0	1	0	2	0	4	0	3	0	1	0	2	0	4	0	3	0	1	**2**
h_7: d_i	d_{18}	d_1	d_8	d_{15}	d_{22}	d_5	d_{12}	d_{19}	d_2	d_9	d_{16}	d_{23}	d_6	d_{13}	d_{20}	d_3	d_{10}	d_{17}	d_0	d_7	d_{14}	d_{21}	d_4	d_{18}
F_7: сдв.	**1**	**4**	4	0	3	4	3	2	2	0	4	2	4	1	1	0	2	1	2	3	3	0	1	**1**
ГМВП																								
$F_г$	3	4	3	0	1	4	4	2	4	0	3	2	2	1	2	0	4	1	1	3	1	0	2	3

Для проверки соответствия функции корреляции полученной ГМВ-последовательности выражению (6) в метрике Ли определены приведенные в таблице 6 расстояния D для сдвигов $\lambda=1$, $\lambda=2$, на основании которых вычислены значения корреляционной функции. Расстояние D определяется как арифметическая сумма символов в соответствующей строке таблицы: $D(\lambda=1) = D(\lambda=2) = 30$. Тогда значения ПАКФ, в соответствии с (6), равны $R(\lambda=1) = R(\lambda=2) = 24\text{-}4*30/5 = 0$, что соответствует выражению (8).

Таблица 6. Корреляция ГМВ-последовательности для двух циклических сдвигов

	Символы ГМВ-последовательности $F_г$ и расстояния D для сдвигов $\lambda=1$, $\lambda=2$																							
$F_г$	3	4	3	0	1	4	4	2	4	0	3	2	2	1	2	0	4	1	1	3	1	0	2	3
$F_г(\lambda=1)$	3	3	4	3	0	1	4	4	2	4	0	3	2	2	1	2	0	4	1	1	3	1	0	2
$D(\lambda=1)$	0	1	1	2	1	2	0	2	2	1	2	1	0	1	1	2	1	2	0	2	2	1	2	1
$F_г(\lambda=2)$	2	3	3	4	3	0	1	4	4	2	4	0	3	2	2	1	2	0	4	1	1	3	1	0
$D(\lambda=2)$	1	1	0	1	2	1	2	2	0	2	1	2	1	1	0	1	2	1	2	2	0	2	1	2

Таким образом, для каждой из четырех базисных М-последовательностей с периодом $N = 24$ (в поле $GF(5^2)$ четыре прими-

тивных полинома) можно сформировать только по одной ГМВ-последовательности с ЭЛС $l_s = 4$. Это определяется тем, что в простом поле GF(5) существует всего два примитивных элемента.

Например, для примитивного полинома $h_{19}(x) = x^2+3x+3$, на основании которого формируется базисная М-последовательность, полиномы-сомножители проверочного полинома ГМВ-последовательности определяются следующим образом. Корнем полинома $h_{c1}(x)$ будет элемент $\alpha^{19*3 \bmod 24} = \alpha^9$. Тогда $h_{c1}(x) = h_9(x) = x^2+2$. Корнем $h_{c2}(x)$ будет элемент $\alpha^{19*7 \bmod 24} = \alpha^{13}$. Тогда $h_{c2}(x) = h_{13}(x) = x^2+4x+2$.

Проверочный полином ГМВ-последовательности будет иметь вид:

$$h_c(x) = h_{c1}(x) h_{c2}(x) = h_9(x) h_{13}(x) = \left(x^2+2\right)\left(x^2+4x+2\right). \qquad (17)$$

Полином $h_{c1}(x) = h_9(x) = x^2+2$ (таблица 1) является непримитивным, период его корней α^9 и α^{21} равен 8. Полином $h_{c2}(x) = h_{13}(x) = x^2+4x+2$ является примитивным, период его корней α^{13} и α^{17} равен 24.

Начальные состояния регистров сдвига можно определить как из символов c_i новой базисной М-последовательности с полиномом $h_{мп}(x) = h_{19}(x) = x^2+3x+3$: (c_0, c_3) и (c_{18}, c_1), так и из символов исходной базисной М-последовательности: $(d_0, d_{3*19 \bmod 24}) = (d_0, d_9) = (2,0)$ и $(d_{18*19 \bmod 24}, d_{1*19}) = (d_6, d_{19}) = (4,2)$.

4. Формирование ГМВ-последовательности с периодом $N = 5^4-1 = 624$.

4.1. Общая часть процедуры формирования. Формирование пятеричных ГМВ-последовательностей осуществляется в расширенном поле $GF[(p^m)^n] = GF[(5^2)^2] = GF(5^4)$.

Построение поля $GF(5^4)$ выполняется по примитивному полиному $f(x) = x^4+x^2+2x+2$, одним из корней которого является примитивный элемент $\alpha = a$. В таблице 7 показан фрагмент построения поля $GF(5^4)$.

Таблица 7. Фрагмент построения конечного поля $GF(5^4)$

Формы элементов поля		Минимальный полином	Период	Корни	След $tr_{4,1}\,\alpha^i$
Степенная	Векторная				
α^0	0001	$h_0(x)=x+4$	1	α^0	4
α^1	0010	$h_1(x)=x^4+x^2+2x+2$	624	$\alpha^1, \alpha^5, \alpha^{25}, \alpha^{125}$	0
α^2	0100	$h_2(x)=x^4+2x^3+4$	312	$\alpha^2, \alpha^{10}, \alpha^{50}, \alpha^{250}$	3
α^3	1000	$h_3(x)=x^4+x^3+2x^2+x+3$	208	$\alpha^3, \alpha^{15}, \alpha^{75}, \alpha^{375}$	4
α^4	0433	$h_4(x)=x^4+x^3+3x^2+1$	156	$\alpha^4, \alpha^{20}, \alpha^{100}, \alpha^{500}$	4
α^5	4300	$h_1(x)=x^4+x^2+2x+2$	624	$\alpha^5, \alpha^{25}, \alpha^{125}, \alpha^1$	0
α^{622}	3233	$h_{622}(x)=x^4+3x+4$	312	$\alpha^{622}, \alpha^{614}, \alpha^{574}, \alpha^{374}$	0
α^{623}	2024	$h_{623}(x)=x^4+x^3+3x^2+3$	624	$\alpha^{623}, \alpha^{619}, \alpha^{599}, \alpha^{499}$	4

Формирование базисной М-последовательности с периодом $N = 624$ осуществляется на основании полинома $h_{\text{мп}}(x) = h_1(x) = x^4+x^2+2x+2$ в соответствии с выражением

$$d_{4+i} = 4d_{2+i} + 3d_{1+i} + 3d_{0+i}, i = 0,\ 1,\ldots,\ 619. \tag{18}$$

Для произвольного начального состояния, например 0001, элементы фрагмента базисной М-последовательности (первые и последние строки) записываются в виде матрицы $\boldsymbol{F}_{\text{мп}}$ размерности $[J\times L] = [25\times 27]$ последовательно по строкам:

$$F_{\text{мп}} = \begin{vmatrix} 0 & 0 & 0 & 1 & 0 & 4 & 3 & 4 & 4 & 2 & 2 & 2 & 1 & 0 & 1 & 4 & 2 & 4 & 3 & 4 & 0 & 2 & 1 & 0 & 0 & 4 \\ 3 & 1 & 4 & 0 & 3 & 0 & 4 & 4 & 0 & 3 & 4 & 4 & 0 & 2 & 4 & 0 & 2 & 3 & 0 & 3 & 0 & 1 & 4 & 3 & 4 & 2 \\ 2 & 4 & 1 & 3 & 2 & 2 & 0 & 3 & 2 & 3 & 2 & 2 & 3 & 3 & 4 & 2 & 4 & 4 & 4 & 4 & 0 & 0 & 4 & 2 & 1 & 0 \\ & & & & & & & & & & & & & & & & & & & & & & & & & \\ 2 & 4 & 1 & 1 & 2 & 4 & 4 & 0 & 4 & 4 & 3 & 3 & 1 & 3 & 2 & 4 & 0 & 1 & 3 & 1 & 0 & 1 & 2 & 2 & 1 & 2 \\ 1 & 2 & 3 & 2 & 1 & 3 & 4 & 1 & 3 & 0 & 2 & 2 & 2 & 4 & 0 & 3 & 3 & 4 & 1 & 4 & 0 & 1 & 0 & 1 & 3 & 2 \end{vmatrix}. \tag{19}$$

Столбцы матрицы представляют собой циклические сдвиги ХП_1 с периодом $J = 2^m-1 = 24$. Вычисляется проверочный полином $h_{\text{хп1}}(x) = h_1(x) = x^2+x+2$ (таблицы1). Для всех столбцов матрицы $\boldsymbol{F}_{\text{мп}}$ определяются номера сдвигов ХП_1 и составляется ПФ, представляющее собой вектор из L=26 компонент, с одним прочерком для обозначения нулевого столбца:

$$\begin{aligned} I_{\text{мп}} = (&22,16,4,23,22,11,12,14,11,9,19,19,\\ &23,10,15,11,20,13,5,13,-,0,15,22,4,18). \end{aligned} \tag{20}$$

В качестве нулевого сдвига ХП_1 произвольно выбран первый столбец после столбца из одних нулей.

Для получения матрицы $\boldsymbol{F}_{\text{г}}$ необходимо в соответствии с правилом $\boldsymbol{I}_{\text{мп}}$ (20) столбцы матрицы $\boldsymbol{F}_{\text{мп}}$, являющиеся сдвигами ХП_1, заменить на другие ХП.

В поле $\text{GF}(5^2)$ существует 4 примитивных полинома, по которым могут формироваться ХП. Это полиномы $h_1(x)=x^2+x+2$ с корнем α^1, $h_7(x)=x^2+2x+3$ с корнем α^7, $h_{13}(x) = x^2+4x+2$ с корнем α^{13} и $h_{19}(x)=x^2+3x+3$ с корнем α^{19}. Таким образом, для каждой базисной М-последовательности можно сформировать по три ГМВ-последовательности с различной ЭЛС, определяемой в соответствии с функцией $g(r)$. Параметр r равен показателям степени корней проверочных полиномов. Для двоичного случая функция $g(r)$ определена

в (2). Для недвоичного случая функция $g(r)$ может быть определена как сумма цифр в p-ичном представлении числа r. Таким образом, $g(r_1=1)=1$, $g(r_2=7_{10}=12_5)=3$, $g(r_3=13_{10}=23_5)=5$, $g(r_4=19_{10}=34_5)=7$.

4.2. Формирование ГМВ-последовательности при r=7. В соответствии с правилом формирования (20) заменим столбцы матрицы базисной М-последовательности (19) на сдвиги ХП_2 с $h_7(x)=x^2+2x+3$. В результате получим ГМВП_1 в матричной форме (21):

$$\mathbf{F_{г1}}=\begin{vmatrix} 1&3&2&3&1&2&4&2&2&1&0&0&3&4&2&2&4&0&1&0&0&1&2&1&2&3\\ 4&2&3&1&4&4&2&0&4&1&3&3&1&1&2&4&0&4&2&4&0&3&2&4&3&4\\ 4&2&3&4&4&1&4&4&1&0&4&4&4&1&0&1&3&2&3&2&0&1&0&4&3&3\\ 1&3&2&0&1&0&2&3&0&2&4&4&0&4&4&0&1&2&0&2&0&3&4&1&2&4\\ 3&4&1&1&3&4&0&2&4&4&4&4&1&2&3&4&4&2&2&2&0&0&3&3&1&0 \end{vmatrix}. \quad (21)$$

Для определения проверочного полинома первой ГМВ-последовательности (ГМВП_1) используем алгоритм Берлекемпа — Месси:

$$h_{c1}(x)=x^{12}+3x^{11}+3x^9+x^8+x^7+2x^6+x^2+4x^5+x^4+3x^3+3x^2+2x+2.$$

Таким образом, ЭЛС полученной ГМВП_1 равна l_s=12.

Разложение на неприводимые полиномы-сомножители четвертой степени поля $\text{GF}(5^4)$ (таблицы 7 и 12) имеет следующий вид:

$$h_{c1}(x)=h_{c1}(x)h_{c2}(x)h_{c3}(x)=h_7(x)h_{11}(x)h_{31}(x)\ =(x^4+x^3+x+3)\times$$
$$\times\left(x^4+x^2+2x+3\right)\left(x^4+2x^3+2x^2+3\right).$$

Все три полинома являются примитивными. Формирование ГМВ-последовательности можно аппаратно реализовать суммированием последовательностей с выходов трех регистров сдвига с проверочными полиномами $h_7(x)$, $h_{11}(x)$ и $h_{31}(x)$, начальные состояния которых определяются путем децимации символов базисной М-последовательности (19) с проверочным полиномом $h_{\text{мп}}(x)=h_1(x)=x^4+x^2+2x+2$ по индексам i_{d1}=7, i_{d2}=11 и i_{d3}=31.

Символы на выходах РС ЛОС определяются коэффициентами полиномов $h_7(x)$, $h_{11}(x)$ и $h_{31}(x)$ с помощью рекуррентных выражений:

$$c_{4+i}=2c_{0+i}+4c_{1+i}+4c_{3+i},\ (i=0,\ 1,\ldots,\ 619); \quad (22)$$

$$c_{4+i}=2c_{0+i}+3c_{1+i}+4c_{2+i},\ (i=0,\ 1,\ldots,\ 619); \quad (23)$$

$$c_{4+i}=2c_{0+i}+3c_{2+i}+3c_{3+i},\ (i=0,\ 1,\ldots,\ 619). \quad (24)$$

При формировании недвоичных ГМВП последовательности с выходов регистров могут иметь определенные циклические сдвиги, кратные величине $N/(p-1)$. Поэтому определение начальных состояний РС ЛОС выполним в соответствии с подходом, изложенным для периода N=24.

Значения начальных состояний РС ЛОС определяются путем решения системы линейных уравнений при заданном сегменте пятеричной ГМВП$_1$ (21) длиной 12 символов, например первых символов первой строки. Затем находятся сдвиги М-последовательностей из условия совпадения начальных состояний регистров.

Аналогично (16) составляется система из 12 линейных уравнений вида $x_{ij} + x_{kl} = c_m$, (i,k = 0, 1, 2, 3 — номер регистра сдвига; j,l = 0, 1, 2, 3 — номер ячейки в регистре; m = 0, 1, 2,…, 11 — номер символа ГМВ-последовательности), каждое из которых определяется с помощью (22)-(24). В результате решения данной системы находим следующие значения начальных состояний для регистров сдвига:

$$\begin{aligned} &x_{00}=3; x_{01}=1; x_{02}=3; x_{03}=4; \\ &x_{10}=3; x_{11}=1; x_{12}=3; x_{13}=2; \\ &x_{20}=0; x_{21}=1; x_{22}=1; x_{23}=2. \end{aligned} \tag{25}$$

Для определения сдвигов последовательностей выполним формирование трех М-последовательностей для начальных состояний РС ЛОС, полученных путем децимации символов базисной М-последовательности по индексам i_{d1}=7, i_{d2}=11 и i_{d3}=31.

$$\begin{aligned} &y_{00}=d_0=4; y_{01}=d_7=4; y_{02}=d_{14}=1; y_{03}=d_{21}=1; \\ &y_{10}=d_0=4; y_{11}=d_{11}=0; y_{12}=d_{14}=3; y_{13}=d_{21}=4; \\ &y_{20}=d_0=4; y_{21}=d_{31}=3; y_{22}=d_{62}=0; y_{23}=d_{93}=4. \end{aligned} \tag{26}$$

При этом обязательным условием является формирование базисной М-последовательности в соответствии с (18) по исходным символам (таблица 7):

$$d_0=tr_{4,1}\alpha^0=4, d_1=tr_{4,1}\alpha^1=0, d_2=tr_{4,1}\alpha^2=3, d_3=tr_{4,1}\alpha^3=4. \tag{27}$$

В таблицах 8 и 9 показаны фрагменты базисной М-последовательности F_1, а также М-последовательностей F_7, F_{11} и F_{31} с полиномами $h_7(x)$, $h_{11}(x)$ и $h_{31}(x)$ с начальными состояниями реги-

стров как в соответствии с (25), так и в соответствии с (26). Приведена результирующая ГМВ-последовательность, полученная суммированием трех М-последовательностей с начальными состояниями (25) и совпадающая с (21).

В таблице 8 выделены совпадения символов последовательностей F_7 (4411) и F_{11} (4034) для начальных состояний (25) и (26). Показано, что данные последовательности не имеют сдвига друг относительно друга и начинаются с символа d_{423} базисной М-последовательности.

Таблица 8. Определение сдвигов последовательностей F_7 и F_{11}

	Символы базисной МП с $h_1(x)$ и МП с $h_7(x)$, $h_{11}(x)$ и $h_{31}(x)$																
h_1: d_i	d_0	d_1	d_2	d_3		d_{419}	d_{420}	d_{421}	d_{422}	d_{423}	d_{424}	d_{425}	d_{426}	d_{427}	d_{428}	d_{429}	d_{430}
F_1	4	0	3	4	…	1	1	1	2	0	4	4	2	3	2	0	3
h_7: d_i	d_0	d_7	d_{14}	d_{21}	…	d_{437}	d_{444}	d_{451}	d_{458}	d_{465}	d_{472}	d_{479}	d_{486}	d_{493}	d_{500}	d_{507}	d_{514}
F_7:(34)	**4**	**4**	**1**	**1**	…	0	1	1	0	4	2	0	1	0	4	0	2
F_7:(33)	3	1	3	4	…	4	1	4	3	**4**	**4**	**1**	**1**	3	4	2	2
h_{11}: d_i	d_0	d_{11}	d_{22}	d_{33}	…	d_{241}	d_{252}	d_{263}	d_{274}	d_{285}	d_{296}	d_{307}	d_{318}	d_{329}	d_{340}	d_{351}	d_{362}
F_{11}:*(34)*	**4**	**0**	**3**	**4**	…	3	3	3	4	2	1	1	3	1	2	0	2
F_{11}:*(33)*	3	1	3	2	…	3	0	2	1	**4**	**0**	**3**	**4**	0	0	3	3
h_{31}: d_i	d_0	d_{31}	d_{62}	d_{93}	…	d_{509}	d_{540}	d_{571}	d_{602}	d_9	d_{40}	d_{71}	d_{102}	d_{133}	d_{164}	d_{195}	d_{226}
F_{31}:*(34)*	4	3	0	4	…	2	4	4	2	2	0	4	1	4	0	0	2
F_{31}:*(33)*	0	1	1	2	…	3	1	4	0	3	1	0	3	0	1	3	3
ГМВП					…												
$F_{г1}$:	1	3	2	3	…	0	2	0	4	1	0	4	3	3	0	3	3

В таблице 9 выделено совпадение символов последовательности F_{31} (4304) для начальных состояний (25) и (26). Показано, что при формировании ГМВ-последовательности данная последовательность должна иметь сдвиг вправо относительно последовательностей F_7 и F_{11}, равный (423-579)mod624=468, что соответствует значению $3N/(p\text{-}1)=0{,}75N$.

В этом случае начальные состояния регистров при формировании М-последовательностей F_7 и F_{11} вычисляются через символы базисной М-последовательности без сдвига следующим образом: (d_0, d_7, d_{14}, d_{21})=(4,4,1,1), (d_0, d_{11}, d_{22}, d_{33})=(4,0,3,4).

Начальные состояния при формировании М-последовательности F_{31} вычисляются через символы базисной М-последовательности с учетом сдвига 468, начиная с символа d_i, где i=468*31 mod624=156. Таким образом, начальное состояние регистра будет (d_{156}, d_{187}, d_{218}, d_{249})=(3,1,0,3).

В результате сложения последовательностей F_7, F_{11} и F_{31} по mod5 получается последовательность, совпадающая с матричным представлением ГМВ-последовательности $F_{г1}$ вида (21).

Таблица 9. Определение сдвига последовательности F_{31}

	Символы базисной МП с $h_1(x)$ и МП с $h_7(x)$, $h_{11}(x)$ и $h_{31}(x)$															
h_1: d_i	d_0	d_1	d_2	d_3		d_{575}	d_{576}	d_{577}	d_{578}	d_{579}	d_{580}	d_{581}	d_{582}	d_{583}	d_{584}	d_{585}	d_{586}
F_1	4	0	3	4	…	2	2	2	4	0	3	3	4	1	4	0	1
h_7: d_i	d_0	d_7	d_{14}	d_{21}	…	d_{281}	d_{288}	d_{295}	d_{302}	d_{309}	d_{316}	d_{323}	d_{330}	d_{337}	d_{344}	d_{351}	d_{358}
F_7:(34)	4	4	1	1	…	0	3	3	0	2	1	0	3	0	2	0	1
F_7:(33)	3	1	3	4	…	2	3	2	4	2	2	3	3	4	2	1	1
h_{11}: d_i	d_0	d_{11}	d_{22}	d_{33}	…	d_{85}	d_{96}	d_{107}	d_{118}	d_{129}	d_{140}	d_{151}	d_{162}	d_{173}	d_{184}	d_{195}	d_{206}
F_{11}:(34)	4	0	3	4	…	4	4	4	2	1	3	3	4	3	1	0	1
F_{11}:(33)	3	1	3	2	…	4	0	1	3	2	0	4	2	0	0	4	4
h_{31}: d_i	d_0	d_{31}	d_{62}	d_{93}	…	d_{353}	d_{384}	d_{415}	d_{446}	d_{477}	d_{508}	d_{539}	d_{570}	d_{601}	d_8	d_{39}	d_{70}
F_{31}:(34)	**4**	**3**	**0**	**4**	…	1	2	2	1	1	0	2	3	2	0	0	1
F_{31}:(33)	0	1	1	2	…	4	3	2	0	**4**	**3**	**0**	**4**	0	3	4	4
ГМВП					…												
$F_{г1}$:	1	3	2	3	…	0	1	0	2	3	0	2	4	4	0	4	4

4.3. Формирование ГМВ-последовательности при *r*=13. Формирование выполняется аналогично рассмотренному выше варианту с параметром ***r*=7.** Поэтому приведем только основные результаты. В соответствии с правилом формирования (20) заменим столбцы матрицы базисной М-последовательности (19) на сдвиги ХП_3 с $h_{13}(x)=x^2+4x+2$. В результате получим ГМВП_2 в матричной форме:

$$\mathbf{F_{г2}}=\begin{vmatrix} 0&0&0&4&0&1&3&4&1&3&3&3&4&0&4&1&2&1&2&1&0&2&4&0&0&4\\ 2&4&1&0&2&0&1&1&0&3&4&4&0&3&4&0&3&3&0&3&0&4&4&2&1&3\\ 2&4&1&2&2&3&0&3&3&2&3&3&2&3&1&3&4&1&1&1&0&0&1&2&1&0\\ 2&4&1&4&2&1&4&0&1&1&2&2&4&3&3&1&0&4&2&4&0&1&3&2&1&2\\ 4&3&2&2&4&3&1&4&3&0&2&2&2&1&0&3&2&4&1&4&0&4&0&4&2&3 \end{vmatrix}. \quad (28)$$

В соответствии с алгоритмом Берлекемпа — Месси определяем проверочный полином ГМВП_2:

$$h_{г2}(x)=x^{24}+x^{23}+x^{22}+3x^{21}+x^{20}+2x^{19}+2x^{17}+4x^{15}+$$
$$+4x^{14}+x^{12}+4x^{11}+x^{10}+x^8+3x^7+4x^5+4x^4+x+4.$$

Таким образом, ЭЛС полученной ГМВП_2 равна l_s=24.

Разложение на неприводимые полиномы-сомножители четвертой степени поля $GF(5^4)$ (таблицы 7 и 12) имеет следующий вид:

$$\begin{aligned} h_{г2}(x)&=h_{c1}(x)h_{c2}(x)h_{c3}(x)h_{c4}(x)h_{c5}(x)h_{c6}(x)=\\ &=h_{13}(x)h_{17}(x)h_{37}(x)h_{41}(x)h_{61}(x)h_{157}(x)=\\ &=\left(x^4+x^2+2\right)\left(x^4+x^3+2x^2+x+2\right)(x^4+x^3+2x^2+2)\times\\ &\times\left(x^4+x^3+3x+2\right)\left(x^4+3x^3+3x+2\right)\left(x^4+4x^2+x+2\right). \end{aligned} \quad (29)$$

Все полиномы являются примитивными, кроме полинома $h_{c1}(x) = x^4+x^2+2$, корни которого имеют период, равный 48. Для получения ГМВ-последовательности необходимо сложить по mod5 шесть последовательностей, начальные состояния которых определяются путем децимации символов базисной М-последовательности, сформированной в соответствии с (18), (27) по индексам $i_{d1} = 13$, $i_{d2} = 17$, $i_{d3} = 37$, $i_{d4} = 41$, $i_{d5} = 61$ и $i_{d6} = 157$.

Для определения начальных сдвигов формируемых последовательностей составим систему из 24 линейных уравнений при заданном сегменте пятеричной ГМВ-последовательности (28) длиной 24 символа, например первых символов второй строки. В результате решения системы вида $x_{ij} + x_{kl} = c_m$, ($i,k = 0, 1, \ldots, 5$ — номер регистра сдвига; $j,l = 0, 1, 2, 3$ — номер ячейки в регистре; $m = 0, 1, 2,\ldots, 23$ — номер символа ГМВ-последовательности) находим следующие значения начальных состояний для регистров сдвига:

$$\begin{gathered} x_{00} = 0; x_{01} = 2; x_{02} = 0; x_{03} = 0; \\ x_{10} = 4; x_{11} = 2; x_{12} = 3; x_{13} = 2; \\ x_{20} = 4; x_{21} = 0; x_{22} = 4; x_{23} = 1; \\ x_{30} = 3; x_{31} = 3; x_{32} = 1; x_{33} = 1; \\ x_{40} = 4; x_{41} = 3; x_{42} = 2; x_{43} = 4; \\ x_{50} = 0; x_{51} = 0; x_{52} = 0; x_{53} = 1. \end{gathered} \tag{30}$$

Для определения сдвигов последовательностей выполним формирование одной ПСП и пяти М-последовательностей в соответствии с проверочными полиномами (29) для начальных состояний РС ЛОС, полученных путем децимации символов базисной М-последовательности по индексам $i_{d1} = 13$, $i_{d2} = 17$, $i_{d3} = 37$, $i_{d4} = 41$, $i_{d5} = 61$ и $i_{d6} = 157$:

$$\begin{gathered} y_{00} = d_0 = 4; y_{01} = d_{13} = 0; y_{02} = d_{26} = 3; y_{03} = d_{39} = 0; \\ y_{10} = d_0 = 4; y_{11} = d_{17} = 4; y_{12} = d_{34} = 2; y_{13} = d_{51} = 2; \\ y_{20} = d_0 = 4; y_{21} = d_{37} = 4; y_{22} = d_{74} = 2; y_{23} = d_{111} = 0; \\ y_{30} = d_0 = 4; y_{31} = d_{41} = 4; y_{32} = d_{82} = 1; y_{33} = d_{123} = 0; \\ y_{40} = d_0 = 4; y_{41} = d_{61} = 2; y_{42} = d_{122} = 4; y_{43} = d_{183} = 4; \\ y_{50} = d_0 = 4; y_{51} = d_{157} = 0; y_{52} = d_{314} = 2; y_{53} = d_{471} = 2. \end{gathered} \tag{31}$$

Как и в случае параметра r=7, обязательным условием является формирование базисной М-последовательности в соответствии с (18)

и (27). В таблице 10 показаны фрагменты базисной М-последовательности F_1, а также ПСП F_{13} и М-последовательностей F_{17}, F_{37}, F_{41}, F_{61} и F_{157} с начальными состояниями регистров как в соответствии с (30), так и в соответствии с (31). Приведена результирующая ГМВ-последовательность, полученная суммированием шести последовательностей с начальными состояниями (30) и совпадающая с (28). Выделены совпадения символов F_{13} (4030), F_{17} (4422) и F_{157} (4022) для начальных состояний (30) и (31). Показано, что данные последовательности не имеют сдвига друг относительно друга.

Таблица 10. Определение сдвигов последовательностей F_{13}, F_{17} и F_{157}

	Символы базисной МП с $h_1(x)$ и суммируемых последовательностей																
h_1: d_i	d_0	d_1	d_2	d_3		d_{341}	d_{342}	d_{343}	d_{344}	d_{345}	d_{346}	d_{347}	d_{348}	d_{349}	d_{350}	d_{351}	d_{352}
F_1	4	0	3	4	…	3	3	2	2	1	3	1	1	1	1	0	0
h_{13}: d_i	d_0	d_{13}	d_{26}	d_{39}	…	d_{65}	d_{78}	d_{91}	d_{104}	d_{117}	d_{130}	d_{143}	d_{156}	d_{169}	d_{182}	d_{195}	d_{208}
F_{13}:(40)	**4**	**0**	**3**	**0**	…	0	0	0	2	0	3	0	3	0	1	0	3
F_{13}:(39)	0	2	0	0	…	1	0	4	0	**4**	**0**	**3**	**0**	4	0	0	0
h_{17}: d_i	d_0	d_{17}	d_{34}	d_{51}	…	d_{181}	d_{198}	d_{215}	d_{232}	d_{249}	d_{266}	d_{283}	d_{300}	d_{317}	d_{334}	d_{351}	d_{368}
F_{17}:(40)	**4**	**4**	**2**	**2**	…	0	4	1	1	3	1	0	3	0	2	0	0
F_{17}:(39)	4	2	3	2	…	1	3	2	2	**4**	**4**	**2**	**2**	2	4	1	0
h_{37}: d_i	d_0	d_{37}	d_{74}	d_{111}	…	d_{137}	d_{174}	d_{211}	d_{248}	d_{285}	d_{322}	d_{359}	d_{396}	d_{433}	d_{470}	d_{507}	d_{544}
F_{37}:(40)	4	4	2	0	…	2	4	0	4	2	2	4	4	4	4	0	4
F_{37}:(39)	4	0	4	1	…	0	3	4	0	2	2	1	0	4	2	3	3
h_{41}: d_i	d_0	d_{41}	d_{82}	d_{123}	…	d_{253}	d_{294}	d_{335}	d_{376}	d_{417}	d_{458}	d_{499}	d_{540}	d_{581}	d_{622}	d_{39}	d_{80}
F_{41}:(40)	4	4	1	0	…	4	1	3	0	4	0	4	4	3	0	0	3
F_{41}:(39)	3	3	1	1	…	4	4	2	2	3	3	2	0	0	3	3	2
h_{61}: d_i	d_0	d_{61}	d_{122}	d_{183}	…	d_{209}	d_{270}	d_{331}	d_{392}	d_{453}	d_{514}	d_{575}	d_{12}	d_{73}	d_{134}	d_{195}	d_{256}
F_{61}:(40)	4	2	4	4	…	1	1	3	2	4	2	2	3	2	4	0	3
F_{61}:(39)	4	3	2	4	…	4	2	3	3	2	1	2	2	2	1	2	4
h_{157}: d_i	d_0	d_{157}	d_{314}	d_{471}	…	d_{497}	d_{30}	d_{187}	d_{344}	d_{501}	d_{34}	d_{191}	d_{348}	d_{505}	d_{38}	d_{195}	d_{352}
F_{157}:(40)	**4**	**0**	**2**	**2**	…	1	2	1	2	2	2	3	1	2	4	0	0
F_{157}:(39)	0	0	0	1	…	0	1	0	2	**4**	**0**	**2**	**2**	4	0	3	2
ГМВП					…												
F_{r2}:	0	0	0	4	…	0	3	0	4	4	0	2	1	1	0	2	1

Аналогично можно показать, что последовательности F_{37} и F_{61} при формировании ГМВ-последовательности должны иметь сдвиг 468, а последовательность F_{41} сдвиг 156 вправо относительно последовательностей F_{13}, F_{17} и F_{157}.

Таким образом, начальные состояния регистров при формировании ПСП F_{13} и М-последовательностей F_{17} и F_{157} вычисляются через известные символы базисной М-последовательности без сдвига следующим образом: $(d_0,d_{13},d_{26},d_{39}) = (4,0,3,0)$, $(d_0,d_{17},d_{34},d_{51}) = (4,4,2,2)$, $(d_0,d_{157},d_{314},d_{471}) = (4,0,2,2)$.

Так как значения функций следа для p-сопряженных элементов в поле GF(5^4) одинаковы, то целесообразно в качестве начального со-

стояния регистра сдвига использовать символ базисной М-последовательности с минимальным индексом. Например, для элемента α^{51} p-сопряженными элементами будут α^{255}, α^{27} и α^{135}, а для элемента α^{471} — элементы α^{483}, α^{543} и α^{219}.

Следовательно, вместо символа d_{51} можно использовать символ с минимальным значением индекса d_{27}, а вместо d_{471} символ d_{219}. Данный подход будет использован в дальнейшем при определении начальных состояний РС ЛОС.

Начальные состояния при формировании М-последовательностей F_{37} и F_{61} вычисляются через символы базисной МП с учетом сдвига 468, начиная с символа d_i, где i=468*37 mod 624=468. Таким образом, начальное состояние регистра для М-последовательности F_{37} будет $(d_{468},d_{29},d_{214},d_{123}) = (2,2,1,0)$, а начальное состояние регистра для М-последовательности F_{61} будет $(d_{468},d_{121},d_{118},d_{27}) = (2,1,2,2)$.

Начальное состояние регистра для М-последовательности F_{41} вычисляется с учетом сдвига 156, начинается с символа d_i, где i=156*41 mod 624=156 и равно $(d_{156},d_{197},d_{238},d_{111}) = (3,3,2,0)$.

В результате сложения последовательностей F_{13}, F_{17}, F_{37}, F_{41}, F_{61} и F_{157} по mod5 получается последовательность, совпадающая с матричным представлением ГМВ-последовательности $F_{г2}$ вида (28).

3.4. Формирование ГМВ-последовательностей при r=19. Формирование выполняется аналогично рассмотренным выше вариантам с параметрами r = 7 и r = 13. В соответствии с правилом формирования (20) заменим столбцы матрицы базисной МП (19) на сдвиги $ХП_4$ с $h_{19}(x) = x^2+3x+3$. В результате получим матрицу $ГМВП_3$:

$$\mathbf{F_{г3}} = \begin{vmatrix} 0 & 0 & 0 & 3 & 0 & 2 & 3 & 1 & 2 & 4 & 1 & 1 & 3 & 0 & 3 & 2 & 2 & 3 & 1 & 3 & 0 & 2 & 3 & 0 & 0 & 1 \\ 1 & 3 & 2 & 0 & 1 & 0 & 2 & 3 & 0 & 3 & 1 & 1 & 0 & 4 & 1 & 0 & 1 & 3 & 0 & 3 & 0 & 3 & 1 & 1 & 2 & 4 \\ 2 & 1 & 4 & 1 & 2 & 4 & 0 & 3 & 4 & 4 & 4 & 4 & 1 & 3 & 3 & 4 & 1 & 2 & 2 & 2 & 0 & 0 & 3 & 2 & 4 & 0 \\ & & & & & & & & & & & ... & & & & & & & & & & & & & \\ 2 & 1 & 4 & 2 & 2 & 3 & 1 & 0 & 3 & 2 & 1 & 1 & 2 & 3 & 4 & 3 & 0 & 3 & 4 & 3 & 0 & 4 & 4 & 2 & 4 & 2 \\ 3 & 4 & 1 & 2 & 3 & 3 & 3 & 3 & 3 & 0 & 2 & 2 & 2 & 2 & 0 & 3 & 1 & 1 & 4 & 1 & 0 & 2 & 0 & 3 & 1 & 1 \end{vmatrix}. \quad (32)$$

В соответствии с алгоритмом Берлекемпа — Месси определяем проверочный полином $ГМВП_3$:

$$h_{г3}(x) = x^{40} + 3x^{39} + x^{37} + x^{36} + x^{35} + 3x^{33} + x^{32} + 2x^{31} + x^{29} + 2x^{28} + 4x^{27} + \\ +2x^{26} + 2x^{25} + 4x^{24} + 2x^{23} + 3x^{22} + 3x^{21} + 4x^{20} + x^{19} + 2x^{17} + 3x^{16} + \\ +2x^{15} + 4x^{13} + 3x^{12} + 2x^{10} + 4x^9 + 2x^8 + x^7 + +2x^6 + 3x^5 + x^3 + 2x^2 + 4.$$

Таким образом, ЭЛС ГМВ-последовательности $F_{г3}$ равна l_s=40.

Разложение на неприводимые полиномы-сомножители четвертой степени поля GF(5^4) (таблица 7) имеет следующий вид:

$$\begin{aligned} h_{\text{г}3}(x) = \\ = h_{c1}(x)h_{c2}(x)h_{c3}(x)h_{c4}(x)h_{c5}(x)h_{c6}(x)h_{c7}(x)h_{c8}(x)h_{c9}(x)h_{c10}(x) = \\ = h_{19}(x)h_{23}(x)h_{43}(x)h_{47}(x)h_{67}(x)h_{71}(x)h_{91}(x)h_{163}(x)h_{167}(x)h_{187}(x) = \\ = \left(x^4+3x^3+2x+3\right)\left(x^4+3x^3+4x+3\right)(x^4+4x^3+4x^2+x+3)\times \\ \times(x^4+4x^3+x^2+4x+3)\left(x^4+2x^3+x+3\right)\left(x^4+x^3+4x^2+4x+3\right)\times \\ \times(x^4+2x^2+3)\left(x^4+2x^3+3x+3\right)\left(x^4+4x^2+x+3\right)\left(x^4+4x^3+3x^2+3\right). \end{aligned} \quad (33)$$

Все полиномы являются примитивными, кроме полинома $h_{c7}(x) = x^4+2x^2+3$, корни которого имеют период, равный 48. Для получения ГМВ-последовательности $F_{\text{г}3}$ необходимо сложить по mod5 десять последовательностей, начальные состояния которых определяются путем децимации символов базисной МП (18) и (27) по индексам i_{d1}=19, i_{d2} = 23, i_{d3} = 43, i_{d4} = 47, i_{d5} = 67, i_{d6} = 71, i_{d7} = 91, i_{d8}=163, i_{d9}=167, i_{d10}=187.

Для определения начальных сдвигов формируемых последовательностей составим систему из 40 линейных уравнений при заданном сегменте пятеричной ГМВ-последовательности $F_{\text{г}3}$ (32) длиной 40 символов. В результате решения системы вида $x_{ij} + x_{kl} = c_m$, (i, k = 0, 1, …, 9 — номер регистра сдвига; j, l = 0, 1, 2, 3 — номер ячейки в регистре; m = 0, 1, 2,…, 39 — номер символа ГМВ-последовательности) находим следующие значения начальных состояний для регистров сдвига:

$$\begin{aligned} &x_{00}=4; x_{01}=4; x_{02}=2; x_{03}=3; \\ &x_{10}=4; x_{11}=0; x_{12}=2; x_{13}=3; \\ &x_{20}=3; x_{21}=3; x_{22}=4; x_{23}=3; \\ &x_{30}=2; x_{31}=0; x_{32}=3; x_{33}=2; \\ &x_{40}=1; x_{41}=0; x_{42}=3; x_{43}=3; \\ &x_{50}=4; x_{51}=1; x_{52}=2; x_{53}=1; \\ &x_{60}=0; x_{61}=1; x_{62}=0; x_{63}=0; \\ &x_{70}=2; x_{71}=3; x_{72}=1; x_{73}=1; \\ &x_{80}=1; x_{81}=1; x_{82}=0; x_{83}=4; \\ &x_{90}=4; x_{91}=2; x_{92}=3; x_{93}=3. \end{aligned} \quad (34)$$

Для определения сдвигов последовательностей выполним формирование одной ПСП и девяти М-последовательностей в соответ-

ствии с проверочными полиномами (33) для начальных состояний РС ЛОС, полученных путем децимации символов базисной М-последовательности по индексам i_{d1}= 19, i_{d2}= 23, i_{d3}= 43, i_{d4}= 47, i_{d5}= 67, i_{d6}= 71, i_{d7}= 91, i_{d8}= 163, i_{d9}= 167, i_{d10}= 187:

$$\begin{gathered}
y_{00} = d_0 = 4; y_{01} = d_{19} = 2; y_{02} = d_{38} = 4; y_{03} = d_{57} = 2; \\
y_{10} = d_0 = 4; y_{11} = d_{23} = 2; y_{12} = d_{46} = 4; y_{13} = d_{69} = 1; \\
y_{20} = d_0 = 4; y_{21} = d_{43} = 1; y_{22} = d_{86} = 3; y_{23} = d_{129} = 1; \\
y_{30} = d_0 = 4; y_{31} = d_{47} = 1; y_{32} = d_{94} = 4; y_{33} = d_{141} = 1; \\
y_{40} = d_0 = 4; y_{41} = d_{67} = 3; y_{42} = d_{134} = 4; y_{43} = d_{201} = 4; \\
y_{50} = d_0 = 4; y_{51} = d_{71} = 4; y_{52} = d_{142} = 3; y_{53} = d_{213} = 4. \\
y_{20} = d_0 = 4; y_{21} = d_{91} = 0; y_{22} = d_{182} = 1; y_{23} = d_{273} = 0; \\
y_{30} = d_0 = 4; y_{31} = d_{163} = 3; y_{32} = d_{326} = 4; y_{33} = d_{489} = 3; \\
y_{40} = d_0 = 4; y_{41} = d_{167} = 0; y_{42} = d_{334} = 2; y_{43} = d_{501} = 2; \\
y_{50} = d_0 = 4; y_{51} = d_{187} = 1; y_{52} = d_{374} = 0; y_{53} = d_{561} = 2.
\end{gathered} \tag{35}$$

В таблице 11 показаны фрагменты базисной М-последовательности F_1, М-последовательностей F_{19}, F_{23}, F_{43}, F_{47}, F_{67}, F_{71}, F_{163}, F_{167}, F_{187}, а также ПСП F_{91} с начальными состояниями регистров как в соответствии с (34), так и в соответствии с (35). Приведен фрагмент результирующей ГМВ-последовательности, полученный суммированием десяти последовательностей с начальными состояниями (34) и совпадающий с (32). Выделены совпадения символов F_{19} (4442), F_{23} (4241) и F_{67} (4344) для начальных состояний (34) и (35). Показано, что данные последовательности не имеют сдвига друг относительно друга и начинаются с символа d_{501} базисной М-последовательности.

Таблица 11. Определение сдвигов последовательностей F_{19}, F_{23} и F_{67}

	Символы базисной МП с $h_1(x)$ и суммируемых последовательностей																
h_1: d_i	d_0	d_1	d_2	d_3		d_{497}	d_{498}	d_{499}	d_{500}	d_{501}	d_{502}	d_{503}	d_{504}	d_{505}	d_{506}	d_{507}	d_{508}
F_1	4	0	3	4	…	1	1	4	4	2	1	2	2	2	2	0	0
h_{19}: d_i	d_0	d_{19}	d_{38}	d_{57}	…	d_{83}	d_{102}	d_{121}	d_{140}	d_{159}	d_{178}	d_{197}	d_{216}	d_{235}	d_{254}	d_{273}	d_{292}
F_{19}⊗35)	**4**	**2**	**4**	**2**	…	2	1	1	3	3	1	3	1	1	3	0	0
F_{19}⊗34)	4	4	2	3		4	3	1	1	**4**	**2**	**4**	**2**	3	2	3	4
h_{23}: d_i	d_0	d_{23}	d_{46}	d_{69}	…	d_{199}	d_{222}	d_{245}	d_{268}	d_{291}	d_{314}	d_{337}	d_{360}	d_{383}	d_{406}	d_{429}	d_{452}
F_{23}⊗35)	**4**	**2**	**4**	**1**		2	1	2	2	4	2	0	3	1	1	0	2
F_{23}⊗34)	4	0	2	3		0	0	4	2	**4**	**2**	**4**	**1**	2	2	3	0
h_{43}: d_i	d_0	d_{43}	d_{86}	d_{129}	…	d_{155}	d_{198}	d_{241}	d_{284}	d_{327}	d_{370}	d_{413}	d_{456}	d_{499}	d_{542}	d_{585}	d_4
F_{43}⊗35)	4	1	3	1		3	4	3	1	1	2	3	1	4	1	0	4
F_{43}⊗34)	3	3	4	3		3	4	2	2	1	4	2	4	4	4	3	1

Продолжение таблицы 11

	Символы базисной МП с $h_1(x)$ и суммируемых последовательностей																
h_{47}: d_i	d_0	d_{47}	d_{94}	d_{141}	…	d_{271}	d_{318}	d_{365}	d_{412}	d_{459}	d_{506}	d_{553}	d_{600}	d_{23}	d_{70}	d_{117}	d_{164}
F_{47}:(35)	4	1	4	1		4	3	2	1	0	2	2	2	2	1	0	0
F_{47}:(34)	2	0	3	2		0	1	0	1	2	3	2	3	3	3	2	3
h_{67}: d_i	d_0	d_{67}	d_{134}	d_{201}	…	d_{227}	d_{294}	d_{361}	d_{428}	d_{495}	d_{562}	d_5	d_{72}	d_{139}	d_{206}	d_{273}	d_{340}
F_{67}:(35)	**4**	**3**	**4**	**4**		3	1	3	2	1	2	0	3	4	1	0	2
F_{67}:(34)	1	0	3	3		0	0	4	3	**4**	**3**	**4**	**4**	2	3	3	0
h_{71}: d_i	d_0	d_{71}	d_{142}	d_{213}	…	d_{343}	d_{414}	d_{485}	d_{556}	d_3	d_{74}	d_{145}	d_{216}	d_{287}	d_{358}	d_{429}	d_{500}
F_{71}:(35)	4	4	3	4		2	4	2	1	4	2	2	1	1	1	0	4
F_{71}:(34)	4	1	2	1		1	2	4	1	2	2	4	2	3	2	1	3
h_{91}: d_i	d_0	d_{91}	d_{182}	d_{273}	…	d_{299}	d_{390}	d_{481}	d_{572}	d_{39}	d_{130}	d_{221}	d_{312}	d_{403}	d_{494}	d_{585}	d_{52}
F_{91}:(35)	4	0	1	0		0	0	0	1	0	3	0	1	0	4	0	4
F_{91}:(34)	0	1	0	0		1	0	3	0	1	0	4	0	4	0	0	0
h_{163}: d_i	d_0	d_{163}	d_{326}	d_{489}	…	d_{515}	d_{54}	d_{217}	d_{380}	d_{543}	d_{82}	d_{245}	d_{408}	d_{571}	d_{110}	d_{273}	d_{436}
F_{163}:(35)	4	3	4	3		3	1	4	3	2	1	2	1	4	3	0	0
F_{163}:(34)	2	3	1	1		3	4	2	3	3	1	3	1	1	1	1	2
h_{167}: d_i	d_0	d_{167}	d_{334}	d_{501}	…	d_7	d_{174}	d_{341}	d_{508}	d_{51}	d_{218}	d_{385}	d_{552}	d_{95}	d_{262}	d_{429}	d_{596}
F_{167}:(35)	4	0	2	2		4	4	3	0	2	0	3	3	2	0	0	4
F_{167}:(34)	1	1	0	4		1	0	1	1	3	0	4	4	0	0	4	3
h_{187}: d_i	d_0	d_{187}	d_{374}	d_{561}	…	d_{587}	d_{150}	d_{337}	d_{524}	d_{87}	d_{274}	d_{461}	d_{24}	d_{211}	d_{398}	d_{585}	d_{148}
F_{187}:(35)	4	1	0	2		0	2	0	0	0	4	4	2	0	2	0	3
F_{187}:(34)	4	2	3	3		2	3	4	0	2	3	0	1	0	3	3	1
ГМВП					…												
$F_{\text{ГЗ}}$:	0	0	0	3		0	2	0	4	1	0	1	2	2	0	3	2

Аналогично можно показать, что последовательности F_{43} и F_{91} при формировании ГМВ-последовательности должны иметь сдвиг 312, последовательности F_{47}, F_{71} и F_{187} должны иметь сдвиг 156, а последовательности F_{163} и F_{167} сдвиг 468 вправо относительно последовательностей F_{19}, F_{23} и F_{67}.

Таким образом, начальные состояния регистров при формировании последовательностей F_{19}, F_{23} и F_{67} вычисляются через символы базисной М-последовательности без сдвига следующим образом:

$$(d_0,d_{19},d_{38},d_{57})=(4,2,4,2),(d_0,d_{23},d_{46},d_{69})=(4,2,4,1),$$
$$(d_0,d_{67},d_{46},d_{33})=(4,3,4,4).$$

Начальные состояния при формировании последовательностей F_{43} и F_{91} вычисляются через символы базисной М-последовательности с учетом сдвига 312, начиная с символа d_i, где i=312*43 mod 624=312. Таким образом, начальное состояние регистра для F_{43} будет (d_{312}, d_{71}, d_{118}, d_{213})=(1,4,2,4), а начальное состояние регистра для F_{91} будет (d_{312}, d_{91}, d_{494}, d_{117})=(1,0,4,0).

Начальные состояния М-последовательностей F_{47}, F_{71} и F_{187} вычисляются с учетом сдвига 156, начиная с символа d_i, где

$i = 156*47 \bmod 624 = 468$. Таким образом, начальное состояние регистра для F_{47} будет $(d_{468}, d_{79}, d_{314}, d_{249}) = (2,3,2,3)$, начальное состояние для F_{71} будет $(d_{468}, d_{199}, d_{122}, d_{57}) = (2,2,4,2)$, а начальное состояние для F_{187} будет $(d_{468}, d_{31}, d_{218}, d_{81}) = (2,3,0,1)$.

Начальные состояния М-последовательностей F_{163} и F_{167} вычисляются с учетом сдвига 468, начиная с символа d_i, где $i = 468*163 \bmod 624 = 156$. Таким образом, начальное состояние регистра для F_{163} будет $(d_{156}, d_{319}, d_{194}, d_{21}) = (3,1,3,1)$, а начальное состояние регистра для F_{167} будет $(d_{156}, d_{323}, d_{98}, d_{33}) = (3,0,4,4)$.

В результате сложения рассмотренных последовательностей по mod5 получается последовательность, совпадающая с матричным представлением ГМВ-последовательности $F_{г3}$ вида (32).

Функция автокорреляции ГМВ-последовательностей (21), (28), (32) в метрике Ли определяется через расстояние D, которое для любого сдвига λ равно 750. Тогда значение ПАКФ, в соответствии с (6), равно $R(\lambda) = 624\text{-}4*750/5 = 24$, что согласуется с (8), то есть $R(\lambda) = p^{S\text{-}2}\text{-}1 = 24$.

Так как в поле $GF(5^4)$ существует 48 примитивных полиномов, являющихся проверочными полиномами для различных базисных М-последовательностей, то для периода N=624 можно сформировать по 48 ГМВ-последовательностей для каждого допустимого значения ЭЛС: l_{s1}=12, l_{s2}=24, l_{s3}=40. Всего в соответствии с (3) можно сформировать 144 ГМВ-последовательности.

5. Синтез устройства формирования ГМВ-последовательности. В предыдущем разделе были получены все необходимые исходные данные для синтеза устройства формирования ГМВ-последовательности с периодом N=624 на основе совокупности РС ЛОС. Для построения устройства требуется знание сомножителей $h_{ci}(x)$ проверочного полинома ГМВ-последовательности $h_г(x)$ и значений начальных состояний ячеек регистров сдвига. Требуемые исходные данные для формирования на основе базисной М-последовательности с $h_1(x) = x^4+x^2+2x+2$ для различных допустимых значений ЭЛС приведены в таблице 12.

Исходные данные в таблице 12 позволяют синтезировать устройства формирования для трех типов ГМВ-последовательностей на основе базисной М-последовательности с $h_1(x) = x^4+x^2+2x+2$. При произвольной базисной М-последовательности с примитивным полиномом $h_i(x)$ необходимо индексы полиномов-сомножителей умножить по mod 624 на параметр i, являющийся показателем степени корня $h_i(x)$. В результате получим новую совокупность полиномов-сомножителей $h_{ci}(x)$. Все минимальные полиномы поля $GF(5^4)$ в виде коэффициентов представлены в таблице 13. Для удобства формирования ГМВ-последовательностей примитивные полиномы выделены подчеркиванием. Отсутствие в таб-

лице полинома с вычисленным индексом означает, что данный индекс соответствует показателю степени одного из p-сопряженных элементов поля. Необходимо найти все p-сопряженные элементы и выбрать среди них элемент с минимальным показателем степени, для которого неприводимый полином имеется в таблице 13.

Таблица 12. Исходные данные для синтеза устройств формирования ГМВ-последовательностей

ЭЛС l_s	Полином $h_{ci}(x)$	Начальные состояния ячеек регистра сдвига				ЭЛС l_s	Полином $h_{ci}(x)$	Начальные состояния ячеек регистра сдвига			
		Я$_0$	Я$_1$	Я$_2$	Я$_3$			Я$_0$	Я$_1$	Я$_2$	Я$_3$
12	$h_7(x)$	d_0=4	d_7=4	d_{14}=1	d_{21}=1	40	$h_{19}(x)$	d_0=4	d_{19}=2	d_{38}=4	d_{57}=2
	$h_{11}(x)$	d_0=4	d_{11}=0	d_{22}=3	d_{33}=4		$h_{23}(x)$	d_0=4	d_{23}=2	d_{46}=4	d_{69}=1
	$h_{31}(x)$	d_{156}=3	d_{187}=1	d_{218}=0	d_{249}=3		$h_{43}(x)$	d_{312}=1	d_{71}=4	d_{118}=2	d_{213}=4
24	$h_{13}(x)$	d_0=4	d_{13}=0	d_{26}=3	d_{39}=0		$h_{47}(x)$	d_{468}=2	d_{79}=3	d_{314}=2	d_{249}=3
	$h_{17}(x)$	d_0=4	d_{17}=4	d_{34}=2	d_{27}=2		$h_{67}(x)$	d_0=4	d_{67}=3	d_{46}=4	d_{33}=4
	$h_{37}(x)$	d_{468}=2	d_{29}=2	d_{214}=1	d_{123}=0		$h_{71}(x)$	d_{468}=2	d_{199}=2	d_{122}=4	d_{57}=2
	$h_{41}(x)$	d_{156}=3	d_{197}=3	d_{238}=2	d_{111}=0		$h_{91}(x)$	d_{312}=1	d_{91}=0	d_{494}=4	d_{117}=0
	$h_{61}(x)$	d_{468}=2	d_{121}=1	d_{118}=2	d_{27}=2		$h_{163}(x)$	d_{156}=3	d_{319}=1	d_{194}=3	d_{21}=1
	$h_{157}(x)$	d_0=4	d_{157}=0	d_{314}=2	d_{219}=2		$h_{167}(x)$	d_{156}=3	d_{323}=0	d_{98}=4	d_{33}=4
							$h_{187}(x)$	d_{468}=2	d_{31}=3	d_{218}=0	d_{81}=1

Начальные состояния ячеек Я$_0$ при произвольной базисной М-последовательности не изменяются по отношению к базисной М-последовательности с $h_1(x)$. Начальные состояния остальных ячеек определяются путем децимации символов базисной М-последовательности в соответствии с индексами новой совокупности полиномов-сомножителей.

Таблица 13. Минимальные полиномы поля GF(5^4), $f(x)=x^4+x^2+2x+2$, $\alpha=a$

α^i	$h_i(x)$ $x^4+\ldots x^0$	α^i	$h_i(x)$ $x^4+\ldots x^0$	α^i	$h_i(x)$ $x^4+\ldots x^0$	α^i	$h_i(x)$ $x^4+\ldots x^0$	α^i	$h_i(x)$ $x^4+\ldots x^0$
α^0	00014	α^{41}	**11032**	α^{86}	12434	α^{162}	11234	α^{237}	13432
α^1	**10122**	α^{42}	13444	α^{87}	10313	α^{163}	**12033**	α^{238}	13234
α^2	12004	α^{43}	**14413**	α^{88}	13341	α^{164}	10431	α^{239}	**11113**
α^3	11213	α^{44}	10421	α^{89}	**14022**	α^{167}	**10413**	α^{242}	14144
α^4	11301	α^{46}	11244	α^{91}	10203	α^{168}	14441	α^{243}	10233
α^6	13314	α^{47}	**14143**	α^{92}	13401	α^{169}	10402	α^{244}	11221
α^7	**11013**	α^{48}	13031	α^{93}	11142	α^{172}	14231	α^{247}	10303
α^8	10111	α^{49}	**13012**	α^{94}	11004	α^{173}	**12332**	α^{248}	11101
α^9	13102	α^{52}	00134	α^{96}	11411	α^{174}	11024	α^{249}	12422
α^{11}	**10123**	α^{53}	**12222**	α^{97}	**13322**	α^{182}	00123	α^{312}	00011
α^{12}	12131	α^{54}	14134	α^{98}	11344	α^{183}	11133	α^{313}	**10132**
α^{13}	10102	α^{56}	10231	α^{99}	14123	α^{184}	14331	α^{314}	13004
α^{14}	14444	α^{57}	13342	α^{104}	00141	α^{187}	**14303**	α^{318}	12344

Продолжение таблицы 13

α^i	$h_i(x)$ $x^4+\ldots x^0$	α^i	$h_i(x)$ $x^4+\ldots x^0$	α^i	$h_i(x)$ $x^4+\ldots x^0$	α^i	$h_i(x)$ $x^4+\ldots x^0$	α^i	$h_i(x)$ $x^4+\ldots x^0$
α^{16}	12311	α^{58}	12324	α^{106}	10044	α^{188}	14301	α^{319}	**14043**
α^{17}	**11212**	α^{59}	**12123**	α^{107}	**11023**	α^{189}	12102	α^{323}	**10133**
α^{18}	13044	α^{61}	**13032**	α^{108}	11041	α^{192}	12121	α^{324}	13121
α^{19}	**13023**	α^{62}	10024	α^{109}	**11342**	α^{193}	**12302**	α^{338}	00142
α^{21}	14232	α^{63}	14243	α^{111}	10223	α^{194}	12134	α^{339}	12443
α^{22}	12224	α^{64}	10141	α^{112}	14101	α^{197}	12042	α^{343}	**13203**
α^{23}	**13043**	α^{66}	12014	α^{113}	**14242**	α^{198}	11124	α^{344}	13201
α^{24}	13131	α^{67}	**12013**	α^{114}	12414	α^{199}	**13133**	α^{348}	14411
α^{26}	00112	α^{68}	13241	α^{116}	12401	α^{208}	00101	α^{349}	**14202**
α^{27}	13413	α^{69}	14402	α^{117}	10002	α^{209}	**14312**	α^{364}	00124
α^{28}	12211	α^{71}	**11443**	α^{118}	13424	α^{212}	10341	α^{368}	10221
α^{29}	**13302**	α^{72}	12021	α^{119}	**10443**	α^{213}	11222	α^{369}	12312
α^{31}	**12203**	α^{73}	**13232**	α^{121}	**14012**	α^{214}	14214	α^{373}	**12022**
α^{32}	12201	α^{74}	13334	α^{122}	11114	α^{217}	**11042**	α^{374}	10034
α^{33}	11402	α^{78}	00103	α^{123}	10343	α^{218}	10014	α^{468}	00012
α^{34}	13124	α^{79}	**12433**	α^{124}	10311	α^{219}	13323	α^{469}	**10442**
α^{36}	11441	α^{81}	14112	α^{156}	00013	α^{222}	14034	α^{474}	14224
α^{37}	**11202**	α^{82}	14314	α^{157}	**10412**	α^{223}	**14033**	α^{494}	00133
α^{38}	11414	α^{83}	**13423**	α^{158}	14004	α^{224}	11321	α^{499}	**11303**
α^{39}	10003	α^{84}	14011	α^{159}	12333	α^{234}	00102		

В качестве примера определим проверочные полиномы и начальные состояния регистров сдвига для трех типов ГМВ-последовательностей с ЭЛС l_{s1} =12, l_{s2} =24 и l_{s3} =40, если в качестве базисной используется М-последовательность с полиномом $h_{\text{мп2}}(x)=h_{223}(x)=x^4+4x^3+3x+3$.

Сомножители проверочного полинома ГМВ-последовательности с ЭЛС l_{s2}=24 $h_{\text{г}4}(x)=h_{\text{с}1}(x)\ldots h_{\text{с}6}(x)$ определяются следующим образом. Одним из корней полинома $h_{\text{с}1}(x)$ будет элемент $\alpha^{223*13\bmod 624}=\alpha^{403}$. Тогда $h_{\text{с}1}(x)=h_{403}(x)=h_{91}(x)=x^4+2x^2+3$. Корнем $h_{\text{с}2}(x)$ будет элемент $\alpha^{223*17\bmod 624}=\alpha^{47}$. Тогда $h_{\text{с}2}(x)=h_{47}(x)=x^4+4x^3+x^2+4x+3$. Остальные полиномы находятся аналогично. В результате проверочный полином ГМВ-последовательности будет иметь вид:

$$h_{\text{г}4}(x)=h_{c1}(x)h_{c2}(x)h_{c3}(x)h_{c4}(x)h_{c5}(x)h_{c6}(x)=$$
$$=h_{91}(x)h_{47}(x)h_{71}(x)h_{163}(x)h_{499}(x)h_{67}(x)=$$
$$=(x^4+2x^2+3)\ (x^4+4x^3+x^2+4x+3)(x^4+x^3+4x^2+4x+3)\times$$
$$\times(x^4+2x^3+3x+3)\ (x^4+x^3+3x^2+3)\ (x^4+2x^3+x+3).$$

Полином $h_{c1}(x)=h_{91}(x)=x^4+2x^2+3$ (таблица 13) является непримитивным, период его корней α^{91}, α^{455}, α^{403}и α^{143} равен 48. Остальные полиномы являются примитивными.

Начальные состояния ячеек $Я_0$ регистров сдвига соответствуют таблице 11. В остальных ячейках начальные состояния определяются децимацией символов базисной МП по индексам полиномов $h_{91}(x)$, $h_{47}(x)$, $h_{71}(x)$, $h_{163}(x)$, $h_{499}(x)$, $h_{67}(x)$ с переходом к минимальным индексам для p-сопряженных элементов, так как функции следа для всех p-сопряженных элементов равны между собой.

Например, для полинома $h_{37}(x)$, преобразованного в полином $h_{71}(x)$, символ $d_{468}=2$ остается без изменений. Индексы остальных символов вычисляются путем последовательного увеличения индекса 468 на 71 и перехода к минимальному значению: $d_{468+71}=d_{539}=d_{199}=2$, $d_{468+142}=d_{610}=d_{122}=4$, $d_{468+213}=d_{681\bmod 624}=d_{57}=2$.

Аналогичным образом определяются начальные состояния регистров сдвига для всех типов ГМВП. Результаты сведены в таблице 14.

Таблица 14. Исходные данные для синтеза устройств формирования ГМВ последовательности на основе базисной М-последовательности с полиномом $h_{223}(x)=x^4+4x^3+3x+3$

ЭЛС l_s	Полином $h_{ci}(x)$	Начальные состояния ячеек регистра сдвига				ЭЛС l_s	Полином $h_{ci}(x)$	Начальные состояния ячеек регистра сдвига			
		$Я_0$	$Я_1$	$Я_2$	$Я_3$			$Я_0$	$Я_1$	$Я_2$	$Я_3$
12	$h_{313}(x)$	$d_0=4$	$d_{313}=0$	$d_2=3$	$d_{63}=1$	40	$h_{469}(x)$	$d_0=4$	$d_{469}=0$	$d_{314}=2$	$d_{159}=3$
	$h_{173}(x)$	$d_0=4$	$d_{173}=3$	$d_{194}=3$	$d_{99}=1$		$h_{61}(x)$	$d_0=4$	$d_{61}=2$	$d_{122}=4$	$d_{183}=4$
	$h_{49}(x)$	$d_{156}=3$	$d_{41}=4$	$d_{22}=3$	$d_{87}=0$		$h_{109}(x)$	$d_{312}=1$	$d_{209}=1$	$d_{106}=0$	$d_3=4$
24	$h_{91}(x)$	$d_0=4$	$d_{91}=0$	$d_{182}=1$	$d_{117}=0$		$h_{349}(x)$	$d_{468}=2$	$d_{193}=3$	$d_{214}=1$	$d_{87}=0$
	$h_{47}(x)$	$d_0=4$	$d_{47}=1$	$d_{94}=4$	$d_{81}=1$		$h_{373}(x)$	$d_0=4$	$d_{373}=3$	$d_{122}=4$	$d_{99}=1$
	$h_{71}(x)$	$d_{468}=2$	$d_{199}=2$	$d_{122}=4$	$d_{57}=2$		$h_{209}(x)$	$d_{468}=2$	$d_{53}=3$	$d_{62}=0$	$d_{219}=2$
	$h_{163}(x)$	$d_{156}=3$	$d_{319}=1$	$d_{194}=3$	$d_{21}=1$		$h_{13}(x)$	$d_{312}=1$	$d_{13}=0$	$d_{338}=2$	$d_{39}=0$
	$h_{499}(x)$	$d_{468}=2$	$d_{343}=2$	$d_{218}=0$	$d_{93}=4$		$h_{157}(x)$	$d_{156}=3$	$d_{313}=0$	$d_{94}=4$	$d_3=4$
	$h_{67}(x)$	$d_0=4$	$d_{67}=3$	$d_{46}=4$	$d_{33}=4$		$h_{17}(x)$	$d_{156}=3$	$d_{173}=3$	$d_{38}=4$	$d_{183}=4$
							$h_{89}(x)$	$d_{468}=2$	$d_{197}=3$	$d_{22}=3$	$d_{111}=0$

Устройство формирования ГМВ-последовательность с $l_{s2}=24$ показано на рисунке 3. Оно состоит из шести регистров сдвига, умножители и сумматоры по mod 5 в цепи обратной связи которых расставляются в соответствии с коэффициентами неприводимых полиномов-сомножителей четвертой степени. Начальные состояния ячеек регистров сдвига даны в таблице 14.

Особенность устройств формирования пятеричных ГМВ-последовательностей заключается в том, что начальные состояния всех регистров сдвига однозначно определяются путем децимации символов базисной М-последовательности по соответствующим индексам децимации с учетом начальных циклических сдвигов суммируемых последовательностей.

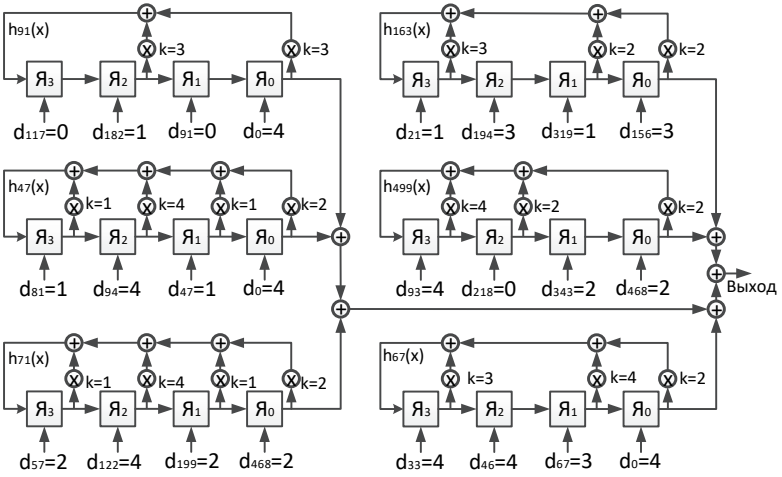

Рис. 3. Устройство формирования ГМВП с ЭЛС l_{s2}=24 на основе базисной МП с $h_{223}(x)=x^4+4x^3+3x+3$

Для каждого примитивного полинома поля GF(5^4) из таблицы 13 могут быть получены начальные состояния регистров сдвига, аналогичные значениям из таблицы 14. При этом в схемной реализации будет изменен только порядок подключения умножителей и сумматоров по mod 5 в цепи обратной связи в соответствии с коэффициентами неприводимых полиномов-сомножителей, также приведенных в таблице 13.

5. Заключение. По корреляционным свойствам ГМВ-последовательности аналогичны М-последовательностям, однако обладают более высокой структурной скрытностью, что определяет предпочтительность их применения в системах передачи дискретной информации, к которым предъявляются повышенные требования как по конфиденциальности, так и по помехозащищенности в условиях радиоэлектронного противодействия.

Переход к недвоичным последовательностям является одним из направлений развития систем передачи информации, обеспечивающим повышение как помехозащищенности телекоммуникационных систем, так и скорости передачи информации.

В настоящее время применению ГМВ-последовательностей, в том числе недвоичных, в системах передачи дискретной информации препятствует отсутствие практически реализуемых алгоритмов и устройств их формирования.

В статье разработан алгоритм формирования пятеричных ГМВ-последовательностей с периодом N=624.

Научная новизна алгоритма заключается в представлении проверочного полинома ГМВ-последовательности в виде произведения неприводимых полиномов, корни которых являются фиксированными степенями корней проверочного полинома базисной М-последовательности, а также в определении начальных символов суммируемых последовательностей, позволяющих однозначно определять их циклические сдвиги.

Практическая значимость алгоритма определяется возможностью синтеза устройств формирования ГМВ-последовательностей только на основе линейных устройств, а именно регистров сдвига с линейными обратными связями, для вычисления начальных состояний которых требуется знание значений символов d_i только одной базисной М-последовательности с полиномом $h_{\text{мп}}(x)=h_1(x)$.

Представленный алгоритм формирования пятеричных ГМВ-последовательностей с периодом N=624 над конечным полем с двойным расширением $\text{GF}[(5^2)^2]$ основан на матричном представлении базисной М-последовательности с примитивным проверочным полиномом $h_{\text{мп}}(x)$. В зависимости от требуемого значения ЭЛС проверочный полином $h_{\text{т}}(x)$ ГМВ-последовательности может быть представлен в виде произведения трех (l_s=12), шести (l_s=24) или десяти (l_s=24) неприводимых над простым полем GF(5) полиномов-сомножителей $h_{ci}(x)$ четвертой степени. Получены соотношения между корнями полинома $h_{\text{мп}}(x)=h_1(x)$ базисной М-последовательности и корнями полиномов-сомножителей $h_{\text{с}i}(x)$ для трех типов ГМВ-последовательностей, на основании которых могут быть определены проверочные полиномы $h_{\text{т}}(x)$ для произвольного примитивного полинома базисной М-последовательности. С учетом того, что в поле $\text{GF}(5^4)$ существует 48 примитивных полиномов, всего можно сформировать 144 пятеричных ГМВ-последовательности с периодом N=624.

Особенностью определения начальных состояний РС ЛОС пятеричных ГМВ-последовательностей по отношению к двоичным является наличие циклических сдвигов для отдельных суммируемых последовательностей. Показано, что данный сдвиг может принимать значения, кратные четверти периода, то есть $N/(p\text{-}1)$. Определены сдвиги для всех типов ГМВ-последовательностей, на основании которых вычислены значения начальных состояний регистров как для базисной М-последовательности с $h_1(x)$, так и для М-последовательности с $h_{223}(x)$. Приведена схема устройства формирования ГМВ-последовательности с ЭЛС l_s=24 для базисной М-последовательности с полиномом $h_{223}(x)$, состоящего из шести регистров сдвига.

ЭЛС пятеричных ГМВ-последовательностей с периодом N=624 может принимать значения 12, 24 и 40, что существенно превышает

аналогичные значения для М-последовательностей. С увеличением периода выигрыш по ЭЛС возрастает. Применение ГМВ-последовательностей при формировании сигналов с расширенным спектром в системах передачи дискретной информации позволяет повысить структурную скрытность сигналов в 3-10 раз по сравнению с использованием М-последовательностей. Платой является увеличение числа регистров с линейной обратной связью, что не является сложной технической задачей.

Алгоритм может найти применение для синтеза устройств формирования ГМВ-последовательностей для помехозащищенных систем передачи дискретной информации, а также для формирования других классов ПСП, допускающих аналитическое представление в конечных полях.

В рамках проведенных исследований не удалось получить аналитического выражения для ЭЛС пятеричных последовательностей, аналогичного выражению (2) для двоичных последовательностей, связывающего параметры m, n и $g(r)$ (значениям $g(r)$=3, 5, 7 соответствуют ЭЛС l_s=12, 24 ,40). Для получения зависимости требуется дополнительная статистика при других значениях параметра p и периода ГМВ-последовательности, что является направлением для дальнейших исследований.

Литература

1. *Скляр Б.* Цифровая связь: Теоретические основы и практическое применение // М.: Вильямс. 2003. 1104 с.
2. *Ипатов В.П.* Широкополосные системы и кодовое разделение сигналов. Принципы и приложения // М.: Техносфера. 2007. 488 с.
3. *Golomb S.W., Gong G.* Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar // Cambridge University Press. 2005. 438 p.
4. Варакина Л.Е., Шинакова Ю.С. CDMA: прошлое, настоящее, будущее // М.: МАС. 2003. 608 с.
5. *Chung H.B., No J.S.* Linear span of extended sequences and cascaded GMW sequences // IEEE Transactions on Information Theory. 1999. vol. 45. no. 6. pp. 2060–2065.
6. *Rizomiliotis P., Kalouptsidis N.* Results on the nonlinear span of binary sequences // IEEE Transactions on Information Theory. 2005. vol. 51. no. 4. pp. 1555–1563.
7. *Ипатов В.П.* Периодические дискретные сигналы с оптимальными корреляционными свойствами // М.: Радио и связь. 1992. 152 с.
8. *No J.S.* Generalization of GMW sequences and No sequences // IEEE Transactions on Information Theory. 1996. vol. 42. no. 1. pp. 260–262.
9. *Стародубцев В.Г., Бородько Д.Н., Мышко В.В.* Алгоритм формирования ГМВ-последовательностей с периодом N=4095 в системах передачи телеметрической информации // Авиакосмическое приборостроение. 2018. № 5. С. 3–15.
10. *Стародубцев В.Г., Мышко В.В., Ткаченко В.В.* Аппаратная и программная реализация алгоритма формирования последовательностей Гордона–Миллса–Велча // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 3. С. 13–20.
11. *Tsankov T., Trifonov T., Staneva L.* An algorithm for synthesis of phase manipulated signals with high structural complexity // Journal Scientific & Applied Research. 2013. vol. 4. pp. 80–87.

12. *Самойленко Д.В., Еремеев М.А., Финько О.А., Диченко С.А.* Параллельный линейный генератор многозначных псевдослучайных последовательностей с контролем ошибок функционирования // Труды СПИИРАН. 2018. Вып. 4(59). С. 31–61.
13. *Стародубцев В.Г., Чернявских А.Е.* Формирование троичных последовательностей Гордона–Миллса–Велча на основе регистров сдвига // Известия высших учебных заведений. Приборостроение. 2016. Т. 59. № 3. С. 201–210.
14. *Lee W., Kim J.Y., No J.S.* New families of p-ary sequence of period (p↑n–1)/2 with low maximum correlation magnitude // IEICE Transactions on Communications. 2014. vol. 97. no. 11. pp. 2311–2315.
15. *Cho C.M., Kim J.Y., No J.S.* New p-ary sequence families of period (p↑n-1)/2 with good correlation property using two decimated m-sequences // IEICE Transactions on Communications. 2015. vol. 98. no. 7. pp. 1268–1275.
16. *Tasheva Z.* A short survey of p-ary pseudo-random sequences // Journal Scientific & Applied Research. 2014. vol. 2. pp. 17–26.
17. *Liang H., Tang Y.* The cross correlation distribution of a p-ary m-sequence of period p↑m–1 and its decimated sequences by (p↑k+1)(p↑m+1)/4 // Finite Fields and Their Applications. 2015. vol. 31. pp. 137–161.
18. *Zhang T., Li S., Feng T., Ge G.* Some new results on the cross correlation of m-sequences // IEEE Transactions on Information Theory. 2014. vol. 60. no. 5. pp. 3062–3068.
19. *Владимиров С.С., Когновицкий О.С.* Широкополосные сигналы данных с расширением спектра прямой троичной М-последовательностью и их характеристика // Труды учебных заведений связи. 2017. Т. 3. № 3. С. 28–36.
20. *Xia Y., Chen S.* A new family of p-ary sequences with low correlation constructed from decimated sequences // IEEE Transactions on Information Theory. 2012. vol. 58. no. 9. pp. 6037–6046.
21. *Helleseth T., Kumar P.V., Martinsen H.* A new family of ternary sequences with ideal two-level autocorrelation function // Designs, Codes and Cryptography. 2001. vol. 23. no. 2. pp. 157–166.
22. *Tang X.H., Pingzhi Z.F.* A class of pseudonoise sequences over GF(p) with low correlation zone // IEEE Transactions on Information Theory. 2001. vol. 47. no. 4. pp. 1644–1649.
23. *Bedzhev B.Y., Yordanov S.S.* Method for synthesis of large families of signals with low correlation // Journal Scientific & Applied Research. 2012. vol. 2. pp. 13–20.
24. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки // М.: Мир. 1976. 594 с.

Стародубцев Виктор Геннадьевич — канд. техн. наук, доцент, старший преподаватель, кафедра технологий и средств автоматизации обработки и анализа информации космических средств, Военно-космическая академия имени А.Ф. Можайского (ВКА им. А.Ф. Можайского). Область научных интересов: теория передачи сигналов, теория конечных полей, системы сигналов сложной формы, помехоустойчивое кодирование. Число научных публикаций — 80. vgstarod@mail.ru; Ждановская, 13, 197198, Санкт-Петербург, Российская Федерация; р.т.: + 7-812-347-95-65.

Поддержка исследований. Исследования, выполненные по данной тематике, проводились при частичной финансовой поддержке грантов РФФИ (№№ 16-29-09482-офи-м, 17-08-00797, 17-06-00108, 17-01-00139, 17-20-01214, 17-29-07073- офи-м, 18-07-01272, 18-08-01505, 19–08–00989), Госзадания Министерства образования и науки РФ №2.3135.2017/4.6.

DOI 10.15622/sp.2019.18.4.912-948

V. G. STARODUBTSEV

FORMATION OF QUINARY GORDON–MILLS–WELCH SEQUENCES FOR DISCRETE INFORMATION TRANSMISSION SYSTEMS

Starodubtsev V. G., Salukhov V. I. **Formation of Quinary Gordon-Mills-Welch Sequences for Discrete Information Transmission Systems.**

Abstract. An algorithm for the formation of the quinary Gordon-Mills-Welch sequences (GMWS) with a period of N=624 over a finite field with a double extension is proposed. The algorithm is based on a matrix representation of a basic M-sequence (MS) with a primitive verification polynomial and a similar period. The transition to non-binary sequences is determined by the increased requirements for the information content of the information transfer processes, the speed of transmission through communication channels and the structural secrecy of the transmitted messages. It is demonstrated that the verification polynomial of the GMWS can be represented as a product of fourth-degree polynomials-factors that are indivisible over a simple field GF(5). The relations between roots of the polynomial of the basic MS and roots of the polynomials-factors are obtained. The entire list of GMWS with a period N=624 can be formed on the basis of the obtained ratios. It is demonstrated that for each of the 48 primitive fourth-degree polynomials that are test polynomials for basis MS, three GMWS with equivalent linear complexity (ELC) of 12, 24, 40 can be formed. The total number of quinary GMWS with period of N=624 is equal to 144. A device for the formation of a GMWS as a set of shift registers with linear feedbacks is presented. The mod5 multipliers and summators in registers are arranged in accordance with the coefficients of indivisible polynomials-factors. The symbols from the registers come to the adder mod5, on the output of which the GMWS is formed. Depending on the required ELC, the GMWS forming device consists of three, six or ten registers. The initial state of cells of the shift registers is determined by the decimation of the symbols of the basic MS at the indexes of decimation, equal to the minimum of the exponents of the roots of polynomials polynomials-factors. A feature of determining the initial States of the devices for the formation of quinary GMWS with respect to binary sequences is the presence of cyclic shifts of the summed sequences by a multiple of $N/(p-1)$. The obtained results allow to synthesize the devices for the formation of a complete list of 144 quinary GMWS with a period of N=624 and different ELC. The results can also be used to construct other classes of pseudo-random sequences that allow analytical representation in finite fields.

Keywords: Pseudorandom Sequences, Finite Fields, Indivisible, Primitive and Minimal Polynomials, Equivalent Linear Complexity, Decimation, Shift Registers.

Starodubtsev Victor Gennadievich — Ph.D., Associate Professor, Senior Lecturer, Department of Technology and Automation of Information Processing and Analysis, Mozhaisky Military Space Academy. Research interests: Theory of Signal Transmission, Theory of Finite Fields, Complex-Form Signal Systems, Noise-Resistant Coding. The number of publications — 80. vgstarod@mail.ru; 13, Zhdanovskaya str., 197198, St. Petersburg, Russian Federation; office phone: + 7-812-347-95-65.

Acknowledgements. This research is partially supported by RFBR according to the research project No. 16-29-09482-ofi-m, 17-08-00797, 17-06-00108, 17-01-00139, 17-20-01214 , 17-29-07073-ofi-m, 18-07-01272, 18-08-01505, 19–08–00989, the Ministry of Science and Higher Education (Project No. 2.3135.2017 / 4.6).

References

1. Sklar B. *Digital Communications: Fundamentals and Applications.* Prentice Hall. 2001. 1079 p. (Russ. ed.: Skljar B. *Cifrovaja svjaz'. Teoreticheskie osnovy i prakticheskoe primenenie.* M.: Vil'yams. 2003. 1104 p.).
2. Ipatov V.P. *Spread Spectrum and CDMA. Principles and Applications.* John Wiley & Sons. 2005. 488 p. (Russ. ed.: Ipatov V.P. *Shirokopolosnye sistemy i kodovoe razdelenie signalov. Principy i prilozhenija*. M.: Tehnosfera. 2007. 488 p.).
3. Golomb S.W., Gong G. Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar. Cambridge University Press. 2005. 438 p.
4. Varakina L.E., Shinakova Ju.S. *CDMA: proshloe, nastojashhee, budushhee* [CDMA: Past, Present, Future]. M.: MAS. 2003. 608 p. (In Russ.).
5. Chung H.B., No J.S. Linear span of extended sequences and cascaded GMW sequences. *IEEE Transactions on Information Theory*. 1999. vol. 45. no. 6. pp. 2060–2065.
6. Rizomiliotis P., Kalouptsidis N. Results on the nonlinear span of binary sequences. *IEEE Transactions on Information Theory*. 2005. vol. 51. no. 4. pp. 1555–1563.
7. Ipatov V.P. *Periodicheskie diskretnye signaly s optimal'nymi korrelyacionnymi svojstvami* [Periodic discrete signals with optimum correlation properties]. M.: Radio i svyaz'. 1992. 152 p. (In Russ.).
8. No J.S. Generalization of GMW sequences and No sequences. *IEEE Transactions on Information Theory.* 1996. vol. 42. no. 1. pp. 260–262.
9. Starodubtsev V.G., Borod'ko D.N., Myshko V.V. [Algorithm for the formation of GMW-sequences with a period of N=4095 in telemetry information transmission systems]. *Aviakosmicheskoe priborostroenie – Aerospace Instrumentation.* 2018. vol. 5. pp. 3–15. (In Russ.).
10. Starodubtsev V.G., Myshko V.V., Tkachenko V.V. [Hardware and software realization of algorithm of formation of Gordon-Mills-Welch sequences]. *Naukoemkie tehnologii v kosmicheskih issledovanijah Zemli – Hi-tech &Earth Space Research.* 2018. Issue 10. vol. 3. pp. 13–20. (In Russ.).
11. Tsankov T., Trifonov T., Staneva L. An algorithm for synthesis of phase manipulated signals with high structural complexity. *Journal Scientific & Applied Research.* 2013. vol. 4. pp. 80–87.
12. Samoylenko D.V., Eremeev M.A., Finko O.A., Dichenko S.A. [Parallel Linear Generator of Multivalued Pseudorandom Sequences with Operation Errors Control]. *Trudy SPIIRAN – SPIIRAS Proceedings.* 2018. vol. 4(59). pp. 31–61. (In Russ.).
13. Starodubtsev V.G., Chernjavskih A.E. [Generation of ternary Gordon-Mills-Welch sequences on the base of shift registers]. *Izvestiya vysshih uchebnyh zavedenij. Priborostroenie – Journal of Instrument Engineering.* 2016. Issue 59. vol. 3. pp. 201–210. (In Russ.).
14. Lee W., Kim J.Y., No J.S. New families of p-ary sequence of period (p↑n–1)/2 with low maximum correlation magnitude. *IEICE Transactions on Communications*. 2014. vol. 97. no. 11. pp. 2311–2315.
15. Cho C.M., Kim J.Y., No J.S. New p-ary sequence families of period (p↑n-1)/2 with good correlation property using two decimated m-sequences. *IEICE Transactions on Communications.* 2015. vol. 98. no. 7. pp. 1268–1275.
16. Tasheva Z. A short survey of p-ary pseudo-random sequences. *Journal Scientific & Applied Research.* 2014. vol. 2. pp. 17–26.
17. Liang H., Tang Y. The cross correlation distribution of a p-ary m-sequence of period p↑m–1 and its decimated sequences by (p↑k+1)(p↑m+1)/4. *Finite Fields and Their Applications*. 2015. vol. 31. pp. 137–161
18. Zhang T., Li S., Feng T., Ge G. Some new results on the cross correlation of m-sequences. *IEEE Transactions on Information Theory.* 2014. vol. 60. no. 5. pp. 3062–3068.

19. Vladimirov S.S., Kognovickij O.S. [Wideband data signals with extension of the spectrum of the direct ternary M-sequence and their characteristics]. *Trudy uchebnyh zavedenij svjazi – Proceedings of educational communications institutions.* 2017. Issue 3. vol. 3. pp. 28–36. (In Russ.).
20. Xia Y., Chen S. A new family of p-ary sequences with low correlation constructed from decimated sequences. *IEEE Transactions on Information Theory*. 2012. vol. 58. no. 9. pp. 6037–6046.
21. Helleseth T., Kumar P.V., Martinsen H. A new family of ternary sequences with ideal two-level autocorrelation function. *Designs, Codes and Cryptography*. 2001. vol. 23. no. 2. pp. 157–166.
22. Tang X.H., Pingzhi Z.F. A class of pseudonoise sequences over GF(p) with low correlation zone. *IEEE Transactions on Information Theory*. 2001. vol. 47. no. 4. pp. 1644–1649.
23. Bedzhev B.Y., Yordanov S.S. Method for synthesis of large families of signals with low correlation. *Journal Scientific & Applied Research.* 2012. vol. 2. pp. 13–20.
24. Peterson W.W., Weldon E.J. *Error-correcting Codes.* MIT press. 1972. 588 p. (Russ. ed.: Peterson W.W., Weldon E.J. *Kody, ispravljajushhie oshibki*. M.: Mir. 1976. 594 p.).