

ТЕОРИЯ И МЕТОДЫ ОБРАБОТКИ СИГНАЛОВ

УДК 519.725;512.62

МЕТОД СИНТЕЗА ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА–МИЛЛСА–ВЕЛЧА ДЛЯ СИСТЕМ ПЕРЕДАЧИ ДИСКРЕТНОЙ ИНФОРМАЦИИ

© 2020 г. В. Г. Стародубцев^{a, b, *}^aВоенно-космическая академия имени А.Ф. Можайского,
ул. Ждановская, 13, Санкт-Петербург, 197198 Российская Федерация^bСанкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Кронверкский пр., 49, Санкт-Петербург, 197101, Российская Федерация

*E-mail: vgstarod@mail.ru

Поступила в редакцию 05.09.2018 г.

После доработки 29.11.2018 г.

Принята к публикации 22.03.2019 г.

Рассмотрен метод синтеза последовательностей Гордона–Миллса–Велча (ГМВП) над расширенным полем $GF(2^m)^n$, основанный на взаимосвязи корней проверочного полинома $h_{МП}(x)$ базисной М-последовательности (МП) и корней полиномов-сомножителей $h_{ci}(x)$ проверочного полинома $h_{ГМВП}(x)$ ГМВП. Показано, что метод синтеза включает алгоритм определения полиномов $h_{ci}(x)$, основанный на использовании p -сопряженных элементов с нечетными показателями степени для элемента β' , принадлежащего подполю $GF(2^m)$, алгоритм определения начальных состояний построенных по полиномам $h_{ci}(x)$ регистров сдвига, который основан на децимации символов базисной МП, и методику определения полных перечней проверочных полиномов $h_{ГМВП}(x)$ ГМВП для всех примитивных полиномов поля $GF(2^m)^n$, на основе которых формируются базисные МП.

DOI: 10.31857/S0033849420010052

Одним из направлений повышения достоверности передачи дискретной информации по радиоканалам, включая каналы спутниковой связи, является применение сигналов с расширенным спектром, формируемых на основе псевдослучайных последовательностей (ПСП) [1–3]. Данное положение относится к системам связи и управления, включая системы спутниковой связи с кодовым разделением сигналов [4, 5], к системам радионавигации и радиолокации [6, 7], а также к системам мобильной связи [8]. В качестве ПСП широко используются МП, последовательности Голда, малого и большого множеств Касами, а также ГМВП [9–11].

Среди ПСП, обладающих двухуровневой периодической автокорреляционной функцией (ПАКФ), можно выделить МП и ГМВП [12, 13]. При этом ГМВП обладают более высокой структурной скрытностью, что определяет приоритетность их использования в системах передачи дискретной информации, к которым предъявляются повышенные требования по конфиденциальности.

Формирование двоичных ГМВП осуществляется над конечными полями с двойным расширением $GF(2^m)^n = GF(2^s)$ ($s = mn$). Период последо-

вательностей является составным числом, т.е. $N = 2^{mn} - 1$.

Символы d_i ГМВП с периодом $N = 2^{mn} - 1$ определяются выражением [7, 12]

$$d_i = \text{tr}_m[(\text{tr}_{mn,m}(\alpha^i))^r], \quad (1)$$

$$1 \leq r < 2^m - 1, \quad (r, 2^m - 1) = 1,$$

где $\text{tr}_{mn,m}(\cdot)$ – след элемента, принадлежащего полю $GF(2^m)^n$, в расширенном поле $GF(2^m)$; $\text{tr}_m(\cdot)$ – след элемента поля $GF(2^m)$ в простом поле $GF(2)$; $\alpha \in GF(2^m)^n$ – примитивный элемент; r – натуральное число, взаимно простое с порядком мультипликативной группы поля $GF(2^m)$, равным $2^m - 1$.

Структурная скрытность ПСП характеризуется эквивалентной линейной сложностью (ЭЛС), которая для двоичных ГМВП определяется выражением [7, 13]

$$l_s = mn^{g(r)}, \quad (2)$$

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

Количество различных ГМВП $M_{ГМВП}$ определяется как произведение числа примитивных по-

линомов в подполе $GF(2^m)$ на число примитивных полиномов в поле $GF[(2^m)^n]$ [12, 13]

$$M_{\text{ГМВП}} = \left(\frac{\varphi(2^m - 1)}{m} - 1 \right) \frac{\varphi(2^{mn} - 1)}{mn}, \quad (3)$$

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

При формировании ГМВП в соответствии с (1) необходимо построить конечное поле $GF(2^s)$, содержащее 2^s элементов, и найти функции следа для каждого элемента. Среднее число операций сложения и умножения по mod 2 при формировании всех ГМВП с периодом $N = 2^s - 1$ может быть определено выражением $K \approx M_{\text{ГМВП}} s 2^s (s + 2)$. Например, для формирования всех ГМВП с периодом $N = 2^8 - 1 = 255$ необходимо выполнить $K \approx 3 \times 10^5$ операций, а для периода $N = 2^{14} - 1 = 16383$ требуется уже $K \approx 4 \times 10^{10}$ операций.

Для полей $GF[(2^m)^n]$ при $n = 2$ известен алгоритм формирования ГМВП [14, 15], основанный на матричном представлении базисной МП. При использовании данного алгоритма для формирования каждой ГМВП необходимо строить матрицу МП, в которой осуществляется замена столбцов. Среднее число операций с учетом формирования МП равно $K \approx \varphi(2^s - 1) 2^s + \varphi(2^m - 1) 2^{m+1}$. Например, для формирования всех ГМВП с периодом $N = 255$ необходимо выполнить $K \approx 4 \times 10^4$ операций, а для периода $N = 16383$ требуется $K \approx 2 \times 10^8$ операций.

Также известен алгоритм формирования ГМВП с помощью совокупности регистров сдвига с линейной обратной связью (РС ЛОС) [16]. При использовании данного алгоритма для каждого периода ГМВП выполняется вычисление проверочного полинома $h_{\text{ГМВП}}(x)$ с помощью алгоритма Берлекэмпа—Мессе и разложение полученного полинома на сомножители. Среднее число операций с учетом формирования МП и выполнения алгоритма Берлекэмпа—Мессе равно $K \approx s 2^s + \varphi(2^m - 1) 2^{m+1} + 2s^3$. Например, для формирования всех ГМВП с периодом $N = 255$ необходимо выполнить $K \approx 8 \times 10^3$ операций, а для периода $N = 16383$ требуется $K \approx 3 \times 10^5$ операций.

Цель данной статьи — разработать метод синтеза ГМВП, основанный на аналитическом определении полиномов-сомножителей $h_{ci}(x)$ проверочного полинома $h_{\text{ГМВП}}(x)$ ГМВП при формировании последовательностей с произвольным составным периодом $N = 2^{mn} - 1$.

Метод синтеза включает три составляющих: алгоритм определения полиномов-сомножителей $h_{ci}(x)$ проверочного полинома ГМВП, методику определения полных перечней проверочных

полиномов $h_{\text{ГМВП}}(x)$ и алгоритм определения начальных состояний регистров сдвига, построенных по полиномам $h_{ci}(x)$ в устройствах формирования ГМВП.

Основу метода синтеза составляет алгоритм определения полиномов-сомножителей $h_{ci}(x)$, отличительной особенностью которого является то, что общий проверочный полином $h_{\text{ГМВП}}(x)$ ГМВП не вычисляется, а его сомножители $h_{ci}(x)$ определяются непосредственно по значению параметра r .

Вторая составляющая метода — это методика определения полных перечней проверочных полиномов $h_{\text{ГМВП}}(x)$, разработанная в [16, 17]. Основой методики является положение о том, что корни полиномов $h_{ci}(x)$ — сомножителей проверочного полинома $h_{\text{ГМВП}}(x)$ — являются определенными фиксированными степенями корней проверочного полинома $h_{\text{МП}}(x)$ базисной МП, с помощью которой формируется ГМВП.

Третьей составляющей метода является предложенный в [16] алгоритм определения начальных состояний регистров сдвига, входящих в устройство формирования ГМВП, который основан на децимации символов базисной МП по индексам, определяемым соотношением показателей степени корней полинома $h_{\text{МП}}(x)$ базисной МП и корней полиномов-сомножителей $h_{ci}(x)$.

При реализации метода число операций сложения и умножения по mod 2 сокращается, так как не требуется построения расширенного поля, формирования базисной МП и вычисления общего проверочного полинома $h_{\text{ГМВП}}(x)$ ГМВП. Среднее число операций может быть определено как $K = (2^{s-2} + \varphi(2^s - 1))/s$. Например, для формирования всех проверочных полиномов ГМВП с периодом $N = 16383$ необходимо выполнить $K \approx 10^3$ операций.

Научная новизна предлагаемого метода заключается в разработке алгоритма определения полиномов-сомножителей $h_{ci}(x)$, которая проводилась на основе анализа результатов, полученных в [15–17].

Для допустимых значений периода N и параметров m и n расширенного поля $GF[(2^m)^n]$ вид формируемой ГМВП, ЭЛС и перечень сомножителей проверочного полинома полностью определяется значением параметра r в выражении (1). При этом показатели степени корней всех полиномов-сомножителей формируемой ГМВП должны иметь одинаковые значения функции $g(r)$.

Алгоритм определения полиномов-сомножителей $h_{ci}(x)$ основан на том, что для элемента $\beta^r = (\text{tr}_{mn,m}(\alpha^i))^r$, принадлежащего подполю $GF(2^m)$, его p -сопряженные элементы с нечетными пока-

зателями степени являются, во-первых, непосредственно корнями части сомножителей степени $s = mn$ проверочного полинома ГМВП, а во-вторых, выступают в качестве образующих элементов для различных p -сопряженных классов поля $GF[(2^m)^n]$ при вычислении остальных сомножителей $h_{ci}(x)$. Данные элементы рассматриваются как корни полиномов-сомножителей нулевого уровня. Отметим, что для каждого значения r общее число элементов с нечетными показателями степени в подполе $GF(2^m)$, равно значению функции $g(r)$. Например, в подполе $GF(2^5)$ поля $GF[(2^5)^2]$ для значения $r = 13$ p -сопряженными элементами для элемента β^{13} являются элементы $\beta^{26}, \beta^{21}, \beta^{11}, \beta^{22}$. Число элементов с нечетными показателями степени равно значению функции $g(13_{10}) = g(1101_2) = 3$, т.е. это элементы $\beta^{13}, \beta^{21}, \beta^{11}$.

Для определения полиномов первого и более высоких уровней вводится вспомогательный параметр k_i , необходимый для вычисления показателей степени корней данных полиномов:

$$k_i = 2i(2^m - 1), \quad i = 1, 2, \dots, 2^{mn-m-1}. \quad (4)$$

Выражение для параметра k_i получено эмпирическим путем на основе анализа показателей степени корней полиномов-сомножителей для ГМВП с периодами $N = 63, 255, 511, 1023$.

На i -м уровне показатели степени корней полиномов определяются путем сложения показателей нулевого уровня и параметра k_i . При выполнении данной операции могут быть получены показатели степени корней неприводимых полиномов, не являющихся полиномами-сомножителями проверочного полинома ГМВП. Поэтому полученные показатели необходимо проверить, во-первых, по параметру $g(r)$ и, во-вторых, по совпадению с показателями корней полиномов более низкого уровня. Обе проверки являются достаточно тривиальными. Вычисления для более высоких уровней продолжаются до получения общего числа сомножителей $M = l_s/s$ степени s проверочного полинома ГМВП.

Рассмотрим алгоритм определения полиномов-сомножителей $h_{ci}(x)$.

Шаг 1. Ввод исходных данных для формирования ГМВП с требуемыми характеристиками над полем $GF[(2^m)^n]$:

- выбор периода ГМВП $N = 2^{mn} - 1$;
- выбор значений m и n для периодов $N = 2^{mn} - 1$;
- выбор примитивного полинома базисной МП с корнем α^1 ;
- задание ЭЛС l_s ГМВП для выбранного периода с соответствующим числом M полиномов-сомножителей;

– выбор параметра r для заданной ЭЛС со значением $g(r)$.

Шаг 2. Определение полиномов-сомножителей $h_{ci}(x)$ нулевого уровня:

– вычисление p -сопряженных элементов для элемента β^r в подполе $GF(2^m)$;

– выбор элементов с нечетными показателями степени $r_{01}, r_{02}, \dots, r_{0d}$, которые являются корнями искомого полиномов-сомножителей нулевого уровня $h_{c1}(x), h_{c2}(x), \dots, h_{cd}(x)$; общее число элементов с нечетными показателями степени равно значению функции $g(r)$, то есть $d = g(r)$.

Шаг 3. Если $d = M$, то переходим в конец алгоритма, т.е. искомым проверочный полином ГМВП определяется выражением

$$h_r(x) = h_{c1}(x)h_{c2}(x) \cdot \dots \cdot h_{cd}(x). \quad (5)$$

Если $d < M$, то в соответствии с (4) определяются значения вспомогательного параметра k_i , необходимого для вычисления показателей степени корней возможных полиномов-сомножителей первого, второго и более высоких уровней.

Шаг 4. Определение полиномов i -го уровня для $i = 1, 2, 3, \dots$:

– вычисление показателей степени i -го уровня $r_{i1}, r_{i2}, \dots, r_{id}$ для нечетных показателей степени корней полиномов нулевого уровня $r_{01}, r_{02}, \dots, r_{0d}$:

$$\begin{aligned} r_{i1} &= r_{01} + k_i, \\ r_{i2} &= r_{02} + k_i, \\ r_{id} &= r_{0d} + k_i, \end{aligned} \quad (6)$$

– проверка полиномов с вычисленными степенями корней:

а) если $g(r_{il}) \neq d$ ($l = 1, 2, \dots, d$), то полином с данным корнем отбрасывается;

б) если r_{il} ($l = 1, 2, \dots, d$) является показателем степени элемента, являющегося p -сопряженным корнем полинома-сомножителя более низкого уровня, то полином с данным корнем повторно не учитывается;

в) число полиномов i -го уровня, прошедших проверку, обозначается d_i .

Шаг 5. Если $d + \sum d_i = M$, то переходим в конец алгоритма, иначе – к шагу 4.

Шаг 6. Конец алгоритма.

Пример. В качестве примера определим проверочный полином для ГМВП с периодом $N = 1023$ и ЭЛС $l_s = 80$.

Шаг 1. Исходные данные: период $N = 1023$; поле $GF[(2^m)^n] = GF[(2^5)^2]$, т.е. $m = 5, n = 2$; полином базисной МП $h_{МП}(x) = x^{10} + x^3 + 1$; параметр $r = 15_{10} = 111_2$; $d = g(r) = g(15) = 4$; ЭЛС $l_s = 5 \times 2^4 = 80$; число сомножителей $M = 8$.

Шаг 2. Определение полиномов-сомножителей $h_{ci}(x)$ нулевого уровня:

– p -сопряженные элементы в поле $GF(2^5)$ для элемента α^{15} : α^{30} , α^{29} , α^{27} , α^{23} ;

– элементы с нечетными показателями степени $r_{01} = 15$, $r_{02} = 23$, $r_{03} = 27$, $r_{04} = 29$ являются корнями искоемых сомножителей нулевого уровня $h_{c1}(x) = h_{15}(x)$, $h_{c2}(x) = h_{23}(x)$, $h_{c3}(x) = h_{27}(x)$, $h_{c4}(x) = h_{29}(x)$, где нижний числовой индекс здесь и далее соответствует наименьшим показателям степени корней полиномов [18];

Шаг 3. Так как $d = 4 < M = 8$, то определяется значение вспомогательного параметра k_i для вычисления показателей степени корней полиномов первого, второго и более высоких уровней:

$$k_i = 2i(2^5 - 1) = 62i, \quad i = 1, 2, \dots, 16.$$

Шаг 4. Определение полиномов первого уровня для $i = 1$ ($k_1 = 62$):

– показатели степени r_{11} , r_{12} , r_{13} , r_{14} корней полиномов первого уровня:

$r_{11} = r_{01} + k_1 = 15 + 62 = 77$, $g(77) = 4$: полином $h_{77}(x)$ соответствует;

$r_{12} = r_{02} + k_1 = 23 + 62 = 85$; $g(85) = 4$: полином $h_{85}(x)$ соответствует;

$r_{13} = r_{03} + k_1 = 27 + 62 = 89$; $g(89) = 4$: полином $h_{89}(x)$ соответствует;

$r_{14} = r_{04} + k_1 = 29 + 62 = 91$; $g(91) = 5 > 4$: полином $h_{91}(x)$ отбрасывается;

– корни α^{77} , α^{85} , α^{89} не являются p -сопряженными элементами для корней полиномов нулевого уровня, поэтому полиномы с данными корнями являются искомыми сомножителями первого уровня $h_{c5}(x) = h_{77}(x)$, $h_{c6}(x) = h_{85}(x)$, $h_{c7}(x) = h_{89}(x)$;

– число полиномов первого уровня, прошедших проверку, равно $d_1 = 3$.

Шаг 5. Так как $d + d_1 = 7 < M = 8$, то вычисляются полиномы второго уровня.

Шаг 6. Определение полиномов второго уровня для $i = 2$ ($k_2 = 124$):

– вычисление показателей степени r_{21} , r_{22} , r_{23} , r_{24} :

$r_{21} = r_{01} + k_2 = 15 + 124 = 139$, $g(139) = 4$: полином $h_{139}(x)$ соответствует;

$r_{22} = r_{02} + k_2 = 23 + 124 = 147$; $g(147) = 4$: полином $h_{147}(x)$ соответствует;

$r_{23} = r_{03} + k_2 = 27 + 124 = 151$; $g(151) = 5 > 4$: полином $h_{151}(x)$ отбрасывается;

$r_{24} = r_{04} + k_2 = 29 + 124 = 153$; $g(153) = 4$: полином $h_{153}(x)$ соответствует;

– корень α^{139} является p -сопряженным элементом для корня α^{89} , корень α^{153} является p -со-

пряженным элементом для корня α^{147} , поэтому полиномы с данными корнями повторно не учитываются; корень α^{147} не является p -сопряженным элементом для корней полиномов более низкого уровня, поэтому единственным полиномом-сомножителем второго уровня является полином $h_{c8}(x) = h_{147}(x)$, $d_2 = 1$.

Шаг 7. Так как $d + d_1 + d_2 = 8 = M$, то искомым полином ГМВП имеет вид

$$h_{\text{ГМВП}}(x) = h_{15}(x)h_{23}(x)h_{27}(x)h_{29}(x)h_{77}(x)h_{85}(x)h_{89}(x)h_{147}(x). \quad (7)$$

Шаг 8. Конец алгоритма.

Проверочный полином $h_{\text{ГМВП}}(x)$ ГМВП вида (7) совпадает с результатами, полученными в [17] при определении данного полинома с помощью алгоритма, основанного на матричном представлении последовательностей, применении алгоритма Берлекэмп–Месси для вычисления полинома $h_{\text{ГМВП}}(x)$ и разложения его на полиномы-сомножители $h_{ci}(x)$.

Устройство формирования ГМВП с периодом $N = 1023$ и проверочным полиномом (7) показано на рисунке. Приведено четыре РС ЛОС из восьми с полиномами [18]

$$h_5(x) = x^{10} + x^8 + x^7 + x^5 + x^3 + x + 1,$$

$$h_{23}(x) = x^{10} + x^4 + x^3 + x + 1,$$

$$h_{89}(x) = x^{10} + x^7 + x^6 + x^4 + x^2 + x + 1,$$

$$h_{147}(x) = x^{10} + x^7 + x^6 + x^5 + x^3 + x^2 + 1.$$

Начальные состояния регистров определены путем децимации символов базисной МП с $h_{\text{МП}}(x) = h_1(x) = x^{10} + x^3 + 1$ [18] по индексам 15, 23, ..., 89, 147 в соответствии с алгоритмом, разработанным в [16].

Таким образом, в статье разработан метод синтеза ГМВП, основу которого составляет алгоритм определения полиномов-сомножителей $h_{ci}(x)$ проверочного полинома $h_{\text{ГМВП}}(x)$ ГМВП. Алгоритм позволяет вычислять неприводимые полиномы-сомножители без построения базисной МП и определения проверочного полинома ГМВП с использованием итеративного алгоритма Берлекэмп–Месси.

ЭЛС ГМВП превышает ЭЛС МП в 2–10 раз в зависимости от значения периода N и выбранного параметра r . С увеличением периода выигрыш возрастает.

Полученные результаты позволяют применять ГМВП в широкополосных радиоканалах систем передачи дискретной информации, к которым предъявляются повышенные требования по кон-

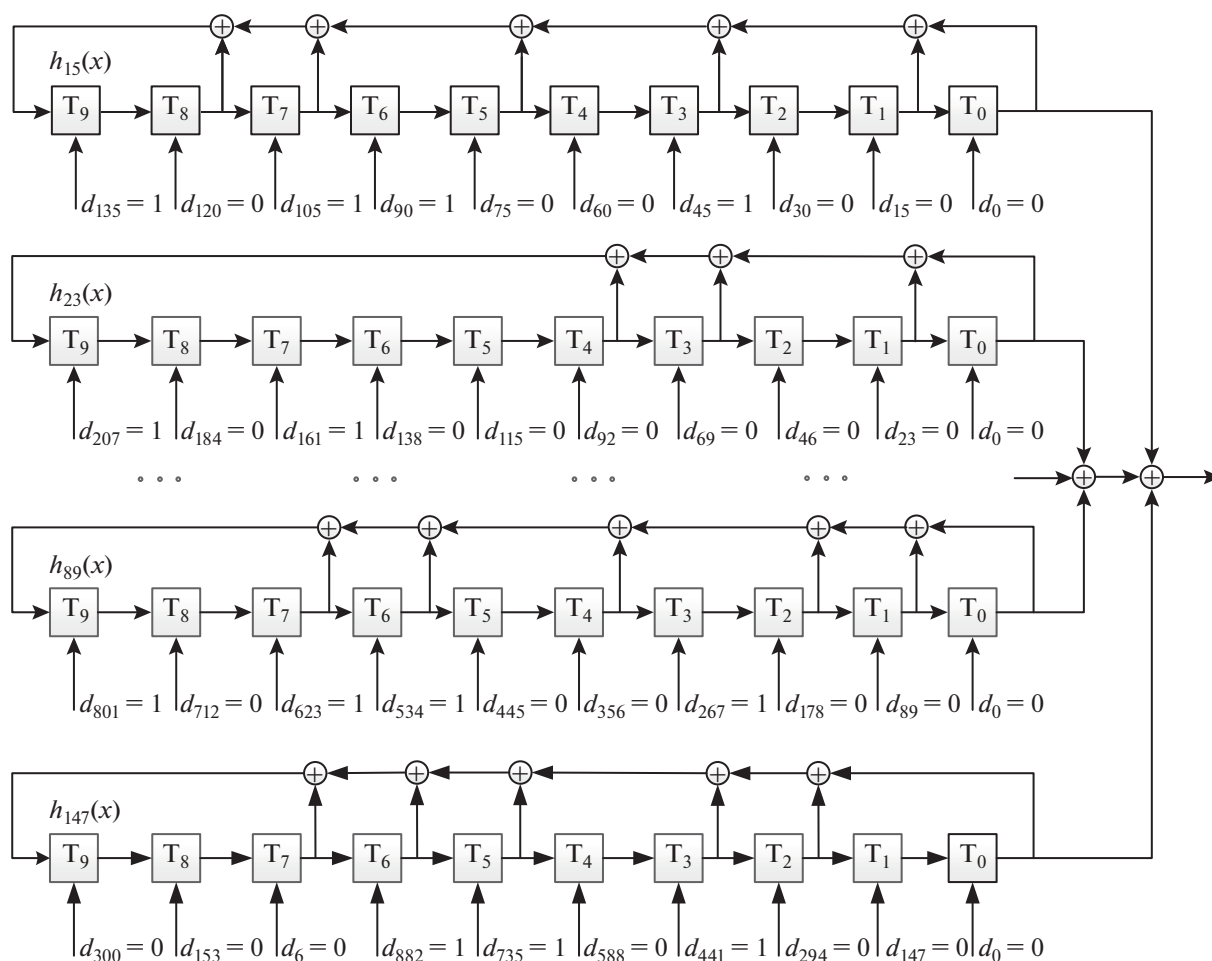


Рис. 1. Схема формирования ГМВП с $N = 1023$ и ЭЛС $L_s = 80$.

фиденциальности, включая требования по повышению их структурной скрытности.

СПИСОК ЛИТЕРАТУРЫ

1. Ипатов В.П. Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992.
2. Вишнеvский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В. Широкополосные беспроводные сети передачи информации. М.: Техносфера, 2005.
3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. 2-е изд. / Пер. с англ. М.: Вильямс, 2003.
4. Ипатов В.П. Широкополосные системы и кодовое разделение сигналов. Принципы и приложения / Пер. с англ. М.: Техносфера, 2007.
5. CDMA: прошлое, настоящее, будущее. М.: МАС, 2003.
6. Wang E., Zhang S., Qing Hu // J. System Simulation. 2008. V. 20. P. 3582.
7. Golomb S.W., Gong G. Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar. Cambridge: Cambridge Univ. Press, 2005.
8. Alasmary W., Zhuang W. // Ad Hoc Networks. 2010. P. 1.
9. Cho Chang-Min, Kim Ji-Youp, No J.S. // IEICE Trans. Commun. 2015. V. E98. № 7. P. 1268.
10. Zhang T., Li S., Feng T., Ge G. // IEEE Trans. 2014. V. IT-60. № 5. P. 3062.
11. Golomb S.W. Two-valued sequences with perfect periodic autocorrelation // IEEE Trans. 1992. V. AES-28. № 2. P. 383.
12. No J.S. // IEEE Trans. 1996. V. IT-42. № 1. P. 260.
13. Chung H., No J.S. // IEEE Trans. 1999. V. IT-45. № 6. P. 2060.
14. Юдачев С.С., Калмыков В.В. // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2012. № 1. URL: <http://elibrary.ru/item.asp?id=17650851>.
15. Стародубцев В.Г. // Изв. вузов. Приборостроение. 2012. Т. 55. № 7. С. 5.
16. Стародубцев В.Г. // Изв. вузов. Приборостроение. 2015. Т. 58. № 6. С. 451.
17. Стародубцев В.Г., Попов А.М. // Изв. вузов. Приборостроение. 2017. Т. 60. № 4. С. 318.
18. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки / Пер. с англ. М.: Мир, 1976.