Научная статья
УДК 512.624.5
https://doi.org/10.31854/1813-324X-2024-10-3-45-58

Кодовое разделение на основе двойного расширения спектра сигнала

Дмитрий Сергеевич Кукунин, kukunin.ds@sut.ru

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

Аннотация

Актуальность: *работа затрагивает проблемы широкополосной модуляции применительно к задачам множественного доступа. Обозначены преимущества кодового уплотнения в процессе расширения спектра сигнала, которое, как показано в работе, является перспективным методом параллельной передачи данных.* ***Целью*** *настоящей работы является, во-первых, повышение эффективности применения адресных последовательностей для идентификации отправителя и получателя информации; во-вторых, организация параллельного процесса передачи данных от одного узла ко многим, обеспечивающая анонимность получателя; и, в-третьих, сохранение низкого пик-фактора сигнала. В* ***задачи*** *работы входит выбор адресных кодовых конструкций, которые на двух этапах расширения спектра сигнала должны решить вопросы идентификации отправителей и получателей информации в сети на физическом уровне. Требуется построить модель системы, которая обеспечит параллельную передачу данных от одного узла ко многим. Важным требованием в такой сети множественного доступа должна стать возможность использования модуляции с наименьшим пик-фактором сигнала.* ***Методы:*** *в данной работе предлагается двухэтапная широкополосная модуляция методом прямого расширения спектра, где каждый узел-отправитель сначала формирует эквивалентный код Голда как сумму последовательностей максимальной длины, адресованных узлам-получателям, а затем использует идентифицирующую его самого адресную последовательность из набора ортогональных сигналов. В работе предложены методы обработки расширяющих спектр последовательностей на основе двойственного базиса поля Галуа, позволяющие достаточно эффективно выделять информацию, предназначенную для каждого получателя.*
Результаты: *предложена модель системы параллельной передачи данных с множественным доступом на основе двухэтапного расширения спектра. Идентификация отправителей и получателей информации осуществляется механизмами формирования адресных сигнально-кодовых конструкций на физическом уровне. Возможен вариант реализации модели с анонимными получателями, когда любой из узлов-получателей не обладает информацией о данных, адресованных другим узлам. Также данная модель не противоречит использованию наиболее помехоустойчивого типа модуляции BPSK (или QPSK в режиме передачи одного разряда), который призван обеспечить предельно низкий пик-фактор сигнала.* ***Новизна.*** *Предложен принципиально новый метод адресации на физическом уровне для сети с параллельной передачей информации, который повышает эффективность использования частотного диапазона.* ***Теоретическая и практическая значимость.*** *Полученные в работе результаты, в перспективе, могут быть использованы при построении различных высоко помехоустойчивых сетей с множественным доступом, где важным требованием является, прежде всего, предельно низкий пик-фактор сигнала источников данных. К таким сетям можно отнести, в частности, сети, образованные роями БПЛА.*

Ключевые слова: *кодовое разделение, последовательность максимальной длины, последовательность Голда, поле Галуа, двойственный базис*

Источник финансирования: *статья подготовлена в рамках прикладных научных исследований СПбГУТ, регистрационный номер 1023031600087-9-2.2.4;2.2.5;2.2.6;1.2.1;2.2.3 в ЕГИСУ НИОКТР.*

Ссылка для цитирования: Кукунин Д.С. Кодовое разделение на основе двойного расширения спектра сигнала // Труды учебных заведений связи. 2024. Т. 10. № 3. С. 45–58. DOI:10.31854/1813-324X-2024-10-3-45-58. EDN:KQSXLR

Original research
https://doi.org/10.31854/1813-324X-2024-10-3-16-23

Code Division Based on Double Spread Spectrum Signal

Dmitriy S. Kukunin, kukunin.ds@sut.ru

The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Annotation

Relevance: *The work addresses the problems of broadband modulation in relation to multiple access problems. The advantages of code multiplexing in the process of expanding the signal spectrum are indicated, which, as shown in the work, is a promising method of parallel data transmission.* ***Purpose:*** *The purpose of this work is, firstly, to increase the efficiency of using address sequences to identify the sender and recipient of information; secondly, to organize a parallel data transmission process from one node to many, ensuring the anonymity of the recipient and, thirdly, maintaining a low peak signal factor.* ***Statement of the problem:*** *The objectives of the work include the selection of address code structures, which, at two stages of expanding the signal spectrum, should solve the issues of identifying senders and recipients of information in the network at the physical level. It is required to build a system model that will ensure parallel data transfer from one node to many. An important requirement in such a multiple access network should be the ability to use modulation with the lowest signal crest factor.* ***Methods:*** *This work proposes two-stage wideband modulation using the direct spread spectrum method, where each sending node first generates an equivalent Gold code as the sum of sequences of maximum length addressed to recipient nodes, and then uses an address sequence identifying itself from set of orthogonal signals. The paper proposes methods for processing spectrum-expanding sequences based on the dual basis of the Galois field, which make it possible to quite effectively isolate information intended for each recipient.* ***Results:*** *A model of a parallel data transmission system with multiple access based on two-stage spectrum expansion is proposed. Identification of senders and recipients of information is carried out by mechanisms for the formation of address signal-code structures at the physical level. It is possible to implement a model with anonymous recipients, when any of the recipient nodes does not have information about the data addressed to other nodes. Also, this model does not contradict the use of the most noise-resistant type of modulation BPSK (or QPSK in single-bit transmission mode), which is designed to provide an extremely low signal crest factor.* ***Novelty****: A fundamentally new method of addressing at the physical level for a network with parallel information transmission is proposed, which increases the efficiency of using the frequency range.* ***Theoretical and practical significance:*** *The results obtained in the work, in the future, can be used in the construction of various highly noise-resistant networks with multiple access, where an important requirement is, first of all, an extremely low crest factor of the data source signal. Such networks include, in particular, networks formed by swarms of UAVs.*

Keywords: *code division, maximum length sequence, Gold sequence, Galois field, dual basis*

Funding*: the article was prepared within the framework of applied scientific research of St. Petersburg State University, registration number 1023031600087-9-2.2.4;2.2.5;2.2.6;1.2.1;2.2.3 in the USISU of R&D.*

For citation: Kukunin D.S. Code Division Based on Double Spread Spectrum Signal. *Proceedings of Telecommunication Universities.* 2024;10(3):45–58. (in Russ.) DOI:10.31854/1813-324X-2024-10-3-45-58. EDN:KQSXLR

Введение

Основной целью процедуры кодового уплотнения на практике является организация множественного доступа по принципу кодового разделения каналов (CDMA, *аббр. от англ.* Code Division Multiple Access) [1, 2], который призван обеспечить обмен данными между абонентами сети, исключив недостатки временного (TDMA, *аббр. от англ.* Time Division Multiple Access) и частотного (FDMA, *аббр. от англ.* Frequency Division Multiple Access) множественного доступа.

Технология FDMA, наиболее востребованная на сегодняшний день в вариации ортогонального частотного разделения (OFDM, *аббр. от англ.* Orthogonal Frequency-Division Multiplexing) [3–6], предполагает использование в качестве абонентских ресурсов полосы частот, временно́й интервал при этом будет общим ресурсом для всех каналов. TDMA, в свою очередь, разделяет абонентов по времени так, что каждый из временны́х интервалов выделяется для передачи блока информации, адресованного определенному абоненту. Таким образом, в случае использования TDMA общим ресурсом является полоса частот, а время, как самый ценный ресурс, становится разделяемым.

Качественное преимущество CDMA заключается в том, что и частотный, и временно́й диапазоны становятся для системы передачи данных общими ресурсами.

Основным инструментом множественного доступа в технологии CDMA являются специальные адресные кодовые последовательности, которые обеспечивают решение двух основных задач [7]:

– увеличение базы сигнала путем расширения его частотного спектра методом прямой последовательности (DSSS, *аббр. от англ.* Direct Sequence Spread Spectrum) [8–12];

– кодовое уплотнение в спектре сигналов, используемых для информационного обмена между множеством абонентов.

Известно, что сигнал с большой базой, то есть широкополосный, обладает лучшей энергетической эффективностью по сравнению с узкополосным сигналом [13, 14]. Немаловажную роль играет также скрытность сигнала, передаваемого в широком спектре частот.

Кодовое разделение каналов CDMA в классическом варианте использует адресные кодовые последовательности, которые в силу своей формы не оказывают влияния друг на друга, или оно сведено к минимуму. Такие кодовые последовательности могут быть объединены в общий сложный сигнал на передаче и разделены соответствующим образом на приеме. При этом каждая адресная последовательность однозначно идентифицирует отправителя информации, что требует в дальнейшем поддержки некоторого протокола идентификации получателя, которому данная последовательность была адресована. Это неизбежно приводит к усложнению архитектуры подобной системы организации множественного доступа вне зависимости, используется ли базовая станция или все абоненты сети работают автономно. Добавим к этому проблему использования в CDMA сложных многоуровневых сигналов, которые так или иначе будут иметь высокое значение пик-фактора.

Целью настоящей работы является, во-первых, повышение эффективности применения адресных последовательностей для идентификации отправителя и получателя информации; во-вторых, организация параллельного процесса передачи данных от одного узла ко многим, обеспечивающая анонимность получателя; и, в-третьих, сохранение низкого пик-фактора сигнала с учетом использования модуляции BPSK или QPSK для передачи одного разряда.

Организация множественного доступа с кодовым уплотнением

В идеале, в качестве адресных последовательностей для кодового уплотнения с последующим разделением следует использовать полностью ортогональные сигналы $A_i(t)$ и $A_j(t)$ периода T, для которых выполняется условие ортонормированности [15]:

$$\frac{1}{T}\sum A_i(t)A_j(t) = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}. \qquad (1)$$

Выполнение условия (1) позволяет реализовать простейшую систему с кодовым уплотнением (рисунок 1), где $A_i(t)$ и $A_j(t)$ действительно не оказывают влияния друг на друга и, следовательно, могут быть использованы в общем частотном и временном диапазонах [7].

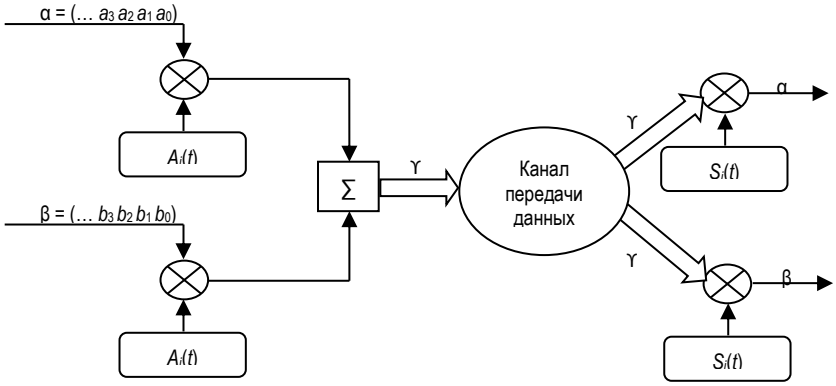

Рис. 1. Схема системы с кодовым уплотнением на основе адресных последовательностей $A_i(t)$ и $A_j(t)$

Fig. 1. The Scheme of Code Division System Based on Address Sequences $A_i(t)$ u $A_j(t)$

Система, построенная на основе схемы, содержит две адресные последовательности: $A_i(t)$ и $A_j(t)$, которые требуется привести к биполярному виду в том случае, если они были двоичными и состояли из символов «0» и «1». Это не будет противоречить дальнейшему применению фазовой модуляции (BPSK или QPSK в режиме передачи одного разряда), которая обеспечит наилучшую помехоустойчивость и низкий пик-фактор сигналов.

Для такого преобразования целесообразно использовать следующее правило [15]:

$$b_i = \begin{cases} +1, & d_i = 0; \\ -1, & d_i = 1; \end{cases} \quad i = 0 \ldots (R-1), \qquad (2)$$

где d_i – двоичный символ исходной последовательности длины R; b_i – соответствующий ему символ, который принимает значение «+1» или «–1». Таким образом, логический нуль кодируется символом «+1», а единица – символом «–1».

Правило (2) не является жестким. Возможен и обратный вариант преобразования, который в последствии должен учитываться на приемной стороне.

Расширение спектра информационных сигналов α и β на схеме (см. рисунок 1) реализуется путем последовательного умножения каждого их элемента на функции $A_i(t)$ и $A_j(t)$, соответственно, что фактически предполагает замену каждого информационного символа «0» на прямую, а символа «1» на инверсную адресную последовательность. Полученный в итоге широкополосный биполярный многоуровневый сигнал на приеме будет представлять собой линейную сумму соответствующих элементов $A_i(t)$ и $A_j(t)$.

Обработку суммарного сигнала на приеме следует рассматривать как независимое вычисление его нормированного скалярного произведения со всеми адресными последовательностями, в том числе с $A_i(t)$ и $A_j(t)$. Полученное в результате такой процедуры значение «+1» или «–1» однозначно определяет соответствующий информационный элемент «0» или «1» [15].

Наиболее известный на сегодняшний день класс ортогональных последовательностей Уолша [16], которые удовлетворяют условию (1) и вполне справляются с задачей кодового уплотнения (см. рисунок 1). Однако, в силу своей природы, эти функции обладают рядом особенностей.

Во-первых, размер ансамбля функций Уолша определяется их периодом $n = 2^i$, где $i = 1, 2, 3, 4, \ldots$, то есть можно сформировать наборы взаимно ортогональных последовательностей лишь в количестве 2, 4, 8, 16, …, длина которых будет соответствовать их числу.

Также необходимо отметить далекие от идеальных автокорреляционные свойства последовательностей Уолша, которые ограничивают их применение в асинхронных системах передачи данных, делая фактически невозможным некогерентные формы приема и, вместе с тем, серьезно повышая требования к цикловой синхронизации [7].

В качестве альтернативы ортогональным функциям Уолша для метода DSSS предлагается использовать рассмотренные в работах [17–19] ортогональные структуры, построенные на основе рекуррентных последовательностей максимальной длины [20].

Общая идея формирования взаимно ортогональных адресных сигналов A_i и A_j (3), полностью удовлетворяющих условию (1) и соответственно пригодных для выполнения задач множественного доступа в CDMA, строится на уникальных свойствах M-последовательностей [7], где M_a, M_b, M_c, M_d – различные последовательности максимальной длины периода L из одного ансамбля, построенные на основе общего минимального многочлена $P(x)$ степени l над полем GF(2^l) и преобразованные в биполярные сигналы по принципу (2).

Выражения (3) фактически предполагают усреднение результата сложения элементов любых двух различных M-последовательностей из ансамбля, представленных в биполярном виде, с элементами их несовпадающих инверсных копий, сдвинутых во времени. Кроме того, частью данного ансамбля также является вырожденная последовательность максимальной длины M_L, которая, в двоичном виде будет содержать L нулей [7].

Таким образом, каждый переданный источником q элемент E информационной последовательности, имеющий значение «0» или «1», будет преобразован в соответствии с правилом (4).

$$\begin{cases} A_i = \dfrac{M_a + \bar{M}_b}{2}; & i, j = 1, 2, \ldots, \left(\dfrac{L+1}{2}\right), \quad a, b, c, d = 0,1,2, \ldots, L, \\ A_j = \dfrac{M_c + \bar{M}_d}{2}; & i \neq j, \quad a \neq b \neq c \neq d, \quad L = 2^l - 1, \quad GF(2^l), \end{cases} . \qquad (3)$$

$$E = \begin{cases} A_q, & \text{«0»}; \\ \bar{A}_q, & \text{«1»}; \end{cases} \quad q = 1,2, \ldots, \left(\frac{L+1}{2}\right), \quad L = 2^l - 1, \quad GF(2^l). \qquad (4)$$

Приведем пример набора ортогональных адресных комбинаций с периодом $L = 15$, построенных по принципу (4) на основе многочлена $P(x) = x^4 + x + 1$.

Для выполнения условий (3) были выбраны пары M-последовательностей в соответствии со своими начальными фазами [7], то есть M_i порождаются начальными элементам ε^i поля GF(2^l), где $i = 0, 1, 2, \ldots, (L - 1)$, при этом M_{15} является вырожденной (5). Не составляет труда убедиться в том, что все комбинации, представленные в (5), ортогональны, а их нормированное на длину периода скалярное произведение подчиняется свойству (1). Таким образом, они вполне годятся для реализации схемы множественного доступа в CDMA (см. рисунок 1). Емкость данного набора адресных последовательностей составляет $(L + 1) / 2$, при этом сами они состоят из биполярных элементов с амплитудами (–1, 0, +1), которые можно в последствии подвергнуть фазовой модуляции, как и предполагалось изначально.

$$
\begin{aligned}
A_1 &= \frac{M_0 + \bar{M}_1}{2} = (0\ \ 0\ +1-1\ 0\ +1\ 0\ -1+1-1+1\ 0\ \ 0\ \ 0\ -1),\\
A_2 &= \frac{M_2 + \bar{M}_3}{2} = (+1-1\ 0\ +1\ 0\ -1+1-1+1\ 0\ \ 0\ \ 0\ -1\ 0\ \ 0),\\
A_3 &= \frac{M_4 + \bar{M}_5}{2} = (0\ +1\ 0\ -1+1-1+1\ 0\ \ 0\ \ 0\ -1\ 0\ \ 0\ +1-1),\\
A_4 &= \frac{M_6 + \bar{M}_7}{2} = (0\ -1+1-1+1\ 0\ \ 0\ \ 0\ -1\ 0\ \ 0\ +1-1\ 0\ +1),\\
A_5 &= \frac{M_8 + \bar{M}_9}{2} = (+1-1+1\ 0\ \ 0\ \ 0\ -1\ 0\ \ 0\ +1-1\ 0\ +1\ 0\ -1),\\
A_6 &= \frac{M_{10} + \bar{M}_{11}}{2} = (+1\ 0\ \ 0\ \ 0\ -1\ 0\ \ 0\ +1-1\ 0+1\ 0\ -1+1-1),\\
A_7 &= \frac{M_{12} + \bar{M}_{13}}{2} = (0\ \ 0\ -1\ 0\ \ 0\ +1-1\ 0\ +1\ 0\ -1+1-1+1\ 0),\\
A_8 &= \frac{M_{14} + \bar{M}_{15}}{2} = (-1\ 0\ \ 0\ \ 0\ -1\ 0\ \ 0\ -1-1\ 0\ -1\ 0\ -1-1-1).
\end{aligned}
\tag{5}
$$

Если рассматривать процедуру такого кодового уплотнения в рамках задачи параллельной передачи данных из некоторой центральной точки множеству устройств, то набор адресных комбинаций увеличивается вплоть до полного периода используемых последовательностей. В частности, в работе [19] описана методика формирования самосинхронизирующегося широкополосного сигнала, который подвергается обработке на приеме двойственным базисом поля Галуа [7, 20] с целью определения начальной фазы заложенной в него синхронизирующей последовательности и, вместе с тем, декодируется подобно помехоустойчивому циклическому коду.

Так или иначе, рассмотренный подход к расширению спектра методом DSSS сохраняет принцип, согласно которому адресные комбинации определяют источник информации, как это было реализовано в классических системах с кодовым разделением каналов. При этом вопросы с адресацией получателя возлагаются на уровни выше. Предлагаемый механизм двойного расширения спектра позволил бы значительно упростить требования к верхним уровням системы передачи данных и фактически решил бы вопрос адресации на физическом уровне.

Таким образом, предварительное расширение спектра методом DSSS позволило бы установить однозначные связи между узлом-получателем и всеми узлами-отправителями информации, обеспечивая вместе с тем одновременную параллельную передачу данных между ними. Для решения данной задачи предлагается использовать эквивалентные коды Голда.

Коды Голда как рекуррентные последовательности

Классический код Голда [7, 20] представляет собой последовательность, формируемую двумя M-последовательностями одного периода $n = 2^k$, которые были построены на базе разных характеристических многочленов вида:

$$
\begin{aligned}
P(x) &= \sum_{i=0}^{k} p_i x^{k-i} = p_0 x^k + \\
&+ p_1 x^{k^{-1}} + \ldots + p_{k_{-1}} x + p_k, \quad p_i \in GF(2).
\end{aligned}
\tag{6}
$$

Приведем пример построения кода Голда $\{\Gamma\} = (\gamma_0\gamma_1\gamma_2\gamma_3\ldots\gamma_{14})$ на основе суммы по mod 2 последовательностей максимальной длины $\{A\} = (a_0a_1a_2a_3\ldots a_{14})$ и $\{B\} = (b_0b_1b_2b_3\ldots b_{14})$ с перио-

дом 15. В качестве порождающих полиномов вида (5) выберем примитивные многочлены, на основе которых не составит труда построить генератор такого кода Голда (рисунок 2), $P_1(x) = x^4 + x + 1$ и $P_2(x) = x^4 + x^3 + 1$.

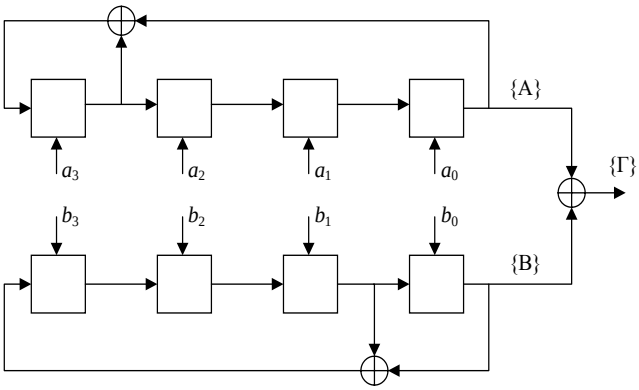

Рис. 2. Генератор последовательности Голда на основе $P_1(x)$ и $P_2(x)$

Fig. 2. Gold Sequence Generator Based on $P_1(x)$ and $P_2(x)$

Так, например, установив произвольные ненулевые начальные значения векторов $(a_0a_1a_2a_3) = (1101)$ и $(b_0b_1b_2b_3) = (0010)$ в схеме (см. рисунок 2), реализуем правило, позволяющее получить на ее выходе последовательность {Г}:

$$\begin{gathered}\{\text{A}\} = (110101111000100)\\ \oplus\\ \underline{\{\text{B}\} = (001000111101011)}\\ \{\Gamma\} = (111101000101111).\end{gathered} \quad (7)$$

Отметим, что, согласно своей природе, последовательности {A} и {B}, используемые в сумме (7), удовлетворяют рекуррентному уравнению с коэффициентами p_i своих многочленов (6):

$$S_i = p_1S_{i-1} + p_2S_{i-2} + \cdots + p_{k-1}S_{i-k+1} + p_kS_{i-k}, \quad p_i \in GF(2), \quad (8)$$

где $[i \pmod{(2^k-1)}] \geq k$.

Параметр k в уравнении (8) определяется старшей степенью полиномов $P_1(x)$ и $P_2(x)$ и в данном примере равен 4. Он же определяет показатель расширенных полей $GF(2^k)$, построенных на основе данных многочленов. Элементы этих полей $GF(2^4)$, в свою очередь, будут соответствовать фазам рекуррентных последовательностей {A} и {B}.

Что касается последовательности {Г}, полученной в результате сложения по правилу (7), то она также будет удовлетворять рекуррентному уравнению, аналогичному (8), но с коэффициентами p_i некоторого нового многочлена $P(x)$:

$$S_i = p_1S_{i-1} + p_2S_{i-2} + \cdots + p_{m-1}S_{i-m+1} + p_mS_{i-m}, \quad p_i \in GF(2), \quad (9)$$

где $[i \pmod{(2^k-1)}] \geq m$.

Параметр m в уравнении (9) определяется старшей степенью многочлена $P(x)$, содержащего произведение минимальных полиномов, на основе которых были построены M-последовательности, входящие в состав кода Голда:

$$P(x) = P_1(x)P_2(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1. \quad (10)$$

Последовательности Голда, построенные на основе рекуррентного соотношения (9) и обрабатываемые соответствующим образом, принято называть эквивалентными [20]. Более того, характеристический многочлен (10), определяющий (9), в общем виде представляет собой произведение V минимальных многочленов $f_i(x)$ и позволяет построить рекуррентную последовательность $\{S\}$ общего вида [7]:

$$S_j = \sum_{i=1}^{V} T(C_i\eta_i^j) = T(C_1\eta_1^j) + T(C_2\eta_2^j) + \cdots + T(C_V\eta_V^j), \quad (11)$$

где η_i – корни соответствующих многочленов $f_i(x)$; $T(C_i\eta^j_i)$ – функция-след от элемента поля Галуа $\alpha^i = C_i\eta^j_i$, которая определяется выражением [7, 20]:

$$T(\alpha^i) = \sum_{j=0}^{k-1}(\alpha^i)^{2^j} = \alpha^i + (\alpha^i)^2 + (\alpha^i)^{2^2} + \ldots + (\alpha^i)^{2^{k-1}}. \quad (12)$$

Коэффициенты C_i в выражении (11) также являются элементами поля Галуа $GF(2^k)$, построенного на основании своего минимального многочлена $f_i(x)$ степени k, и могут быть вычислены по начальному участку $(S_0S_1S_2\ldots S_{m-1})$ рекуррентной последовательности $\{S\}$ следующим образом [7]:

$$C_i = \eta_i^{-\delta}\sum_{j=1}^{m}\omega_{ij}S_{\delta+j-1}, \quad i = 1 \ldots V, \quad (13)$$

где δ – расстояние текущего m-элементного участка относительно начала последовательности $\{S\}$, сформированной на основе выражения (11) через функцию (12).

Коэффициенты ω_{ij} в равенстве (13) также являются элементами поля Галуа $GF(2^k)$, построенного на основании соответствующего многочлена $f_i(x)$, их принято называть базисными или двойственного базиса [7, 20].

Для вычисления базисных коэффициентов может быть использовано выражение [7]:

$$\omega_{i\rho} = \frac{\sum_{l=0}^{m-\rho} p_{m-\rho-l}(\eta_i)^l}{P'(\eta_i)}, \quad \rho = 1, 2, \ldots, m, \quad (14)$$

где m – старшая степень многочлена $P(x)$; $P'(\eta_i)$ – значение его производной в точке, которая соот-

ветствует примитивному элементу η_i поля GF(2^k), построенного на основе соответствующего многочлена $f_i(x)$.

Вернувшись к примеру с последовательностью Голда, состоящей из двух *M*-последовательностей (7), обозначим примитивные элементы ε и μ для двух полей GF(2^4), построенных, соответственно, на основе многочленов $P_1(x)$ и $P_2(x)$. В данном случае формула (14) без труда позволит вычислить базисные коэффициенты $\omega_{1\rho} = \lambda_\rho$ и $\omega_{1\rho} = \upsilon_\rho$ на основе следующих выражений [7]:

$$\lambda_\rho = \frac{\sum_{l=0}^{m-\rho} p_{m-\rho-l}(\varepsilon)^l}{P'(\varepsilon)}, \quad \upsilon_\rho = \frac{\sum_{l=0}^{m-\rho} p_{m-\rho-l}(\mu)^l}{P'(\mu)}, \quad \rho = 1, 2, \dots, m. \tag{15}$$

Так, применяя (15), определим коэффициенты двойственного базиса, которые в данном случае будут постоянными для характеристического многочлена (8):

$$\{\lambda\} = (\varepsilon^5\varepsilon^8\varepsilon^7\varepsilon^9\varepsilon^4\varepsilon^{11}\varepsilon^{10}\varepsilon^6),$$
$$\{\upsilon\} = (\mu^2\mu^{13}\mu^{12}\mu^4\mu^{14}\mu\ 1\ \mu^3). \tag{16}$$

Теперь, обладая наборами элементов (16) из двух полей GF(2^4) и учитывая свойство (11), можем вычислить коэффициенты *C* и *D*, которые, используя выражение $\gamma_j = T(C\varepsilon^j) + T(D\mu^j)$, позволят определить произвольный элемент последовательности Голда {Г}=($\gamma_0\gamma_1\gamma_2\gamma_3 \dots \gamma_{14}$):

$$C = \varepsilon^{-\delta}\sum_{i=1}^{m}\lambda_i\gamma_{\delta+i-1}, \quad D = \mu^{-\delta}\sum_{i=1}^{m}\upsilon_i\gamma_{\delta+i-1}, \tag{17}$$

где δ – расстояние *m*-элементного участка относительно начала {Г}.

Отметим, что элементы *C* и *D* принято считать начальными фазами *M*-последовательностей {A} и {B}, то есть теми элементами своих полей GF(2^4), которые порождают эти последовательности [7, 20]. Задача определения начальных фаз рекуррентных последовательностей {A} и {B} сводится к обработке *m*-элементных участков {Г} по принципу (17).

Произведем такую обработку нескольких последовательных участков {Г} = ($\gamma_0\gamma_1\gamma_2\gamma_3 \dots \gamma_{14}$) длины $m = 8$ и определим значения начальных фаз *M*-последовательностей, составляющих данный код Голда [7].

Нулевой участок ($\gamma_0\gamma_1\gamma_2\gamma_3\gamma_4\gamma_5\gamma_6\gamma_7$) = (11110100):

$$C = \varepsilon^5 + \varepsilon^8 + \varepsilon^7 + \varepsilon^9 + \varepsilon^{11} = \varepsilon^6,$$
$$D = \mu^2 + \mu^{13} + \mu^{12} + \mu^4 + \mu = \mu^{10}.$$

Первый участок ($\gamma_1\gamma_2\gamma_3\gamma_4\gamma_5\gamma_6\gamma_7\gamma_8$) = (11101000):

$$C = \varepsilon^{-1}(\varepsilon^5 + \varepsilon^8 + \varepsilon^7 + \varepsilon^4) = \varepsilon^6,$$
$$D = \mu^{-1}(\mu^2 + \mu^{13} + \mu^{12} + \mu^{14}) = \mu^{10}.$$

Второй участок ($\gamma_2\gamma_3\gamma_4\gamma_5\gamma_6\gamma_7\gamma_8\gamma_9$) = (11010001):

$$C = \varepsilon^{-2}(\varepsilon^5 + \varepsilon^8 + \varepsilon^9 + \varepsilon^6) = \varepsilon^6,$$
$$D = \mu^{-2}(\mu^2 + \mu^{13} + \mu^4 + \mu^3) = \mu^{10}.$$

Третий участок ($\gamma_3\gamma_4\gamma_5\gamma_6\gamma_7\gamma_8\gamma_9\gamma_{10}$) = (10100010):

$$C = \varepsilon^{-3}(\varepsilon^5 + \varepsilon^7 + \varepsilon^{10}) = \varepsilon^6,$$
$$D = \mu^{-3}(\mu^2 + \mu^{12} + 1) = \mu^{10}.$$

Четвертый участок ($\gamma_4\gamma_5\gamma_6\gamma_7\gamma_8\gamma_9\gamma_{10}\gamma_{11}$) = (01000101):

$$C = \varepsilon^{-4}(\varepsilon^8 + \varepsilon^{11} + \varepsilon^6) = \varepsilon^6,$$
$$D = \mu^{-4}(\mu^{13} + \mu + \mu^3) = \mu^{10}.$$

Пятый участок ($\gamma_5\gamma_6\gamma_7\gamma_8\gamma_9\gamma_{10}\gamma_{11}\gamma_{12}$) = (10001011):

$$C = \varepsilon^{-5}(\varepsilon^5 + \varepsilon^4 + \varepsilon^{10} + \varepsilon^6) = \varepsilon^6,$$
$$D = \mu^{-5}(\mu^2 + \mu^{14} + 1 + \mu^3) = \mu^{10}.$$

Полученные результаты говорят о том, что для формирования последовательности Голда были использованы *M*-последовательности с начальными фазами ε^6 и μ^{10}.

Кодовое уплотнение на основе кодов Голда

Рассмотрев пример с классическим кодом Голда, который представляет собой сумму лишь двух *M*-последовательностей, имеет смысл перейти к более интересному примеру, когда выражение (11) включает в себя несколько слагаемых.

Действительно, ничто не мешает построить эквивалентный код Голда, сложив по mod 2 более двух последовательностей максимальной длины, принадлежащих разным ансамблям. Ограничением при этом будет только число характеристических полиномов *V* степени *k* из разложения двучлена $x^n - 1$, где $n = 2^k - 1$.

Согласно принципу разложения $x^n - 1$ на составляющие, число таких многочленов *V* степени *k* будет определяться следующим выражением:

$$V = \frac{\varphi(2^k - 1)}{k}, \tag{18}$$

где $\varphi(2^k - 1)$ – функция Эйлера от $n = 2^k - 1$.

Рассмотрим пример для $k = 5$, когда, согласно формуле (18), многочленов, пригодных для построения поля GF(2^5), будет:

$$V = \varphi(2^k - 1)/k = \varphi(31)/5 = 30/5 = 6,$$

а их *M*-последовательности будут иметь период 31 (таблица 1). Представленные последовательности максимальной длины имеют каноническую форму [20], при этом их начальной фазой в любом поле GF(2^5) является элемент $\eta^0 = 1$. Когда речь заходит о передаче информации при помощи *M*-последовательностей, необходимо обеспечить смещение их фазы на определенное количество разрядов.

ТАБЛИЦА 1. Минимальные многочлены для GF(2^5) и их *M*-последовательности

TABLE 1. Minimum Polynomials for GF(2^5) and Their M-Sequences

Минимальный полином	*M*-последовательность в канонической форме
$P_1(x) = x^5+x^2+1$	$\{S\}_1$ = (10010110011111000110111010100 00)
$P_2(x) = x^5+x^4+x^3+x^2+1$	$\{S\}_2$ = (11111011100010101101000011001 00)
$P_3(x) = x^5+x^3+1$	$\{S\}_3$ = (10000101011101100011111001101 00)
$P_4(x) = x^5+x^3+x^2+x+1$	$\{S\}_4$ = (10010011000010110101000111011 11)
$P_5(x) = x^5+x^4+x^3+x+1$	$\{S\}_5$ = (11101100111000011010100100010 11)
$P_6(x) = x^5+x^4+x^2+x+1$	$\{S\}_6$ = (11101000100101011000011100110 11)

Таким образом, текущая фаза *M*-последовательности $\{S\}_i$, где i = 1, 2, …, 6, однозначно определяет «где содержится информация?» одним из следующих способов:

1) в первых k = 5 разрядах *M*-последовательности $\{S_0S_1S_2S_3S_4\}_i$;

2) в элементе η^j поля GF(2^5), который порождает данную *M*-последовательность $\{S\}_i$.

При этом второй способ имеет две возможные вариации – информация содержится в разрядах вектора, или в показателе степени j вектора, представляющего элемент η^j поля GF(2^k).

Ограничения, которые накладываются на все вышеперечисленные способы представления информации, очевидны. Так, в случае варианта 1 участок $\{S_0S_1S_2S_3S_4\}_i$ для всех i = 1, 2, …, 6 не должен быть полностью нулевым, иначе *M*-последовательность, удовлетворяющая условию (7), также станет нулевой или вырожденной [7]. Это, в свою очередь, приведет к тому, что ее присутствие в общем коде Голда будет равносильно отсутствию.

То же условие невозможности использования нулевого значения информационного вектора характерно и для варианта, когда информация содержится в разрядах вектора. Ведь нулевой элемент поля Галуа также приведет к формированию вырожденной рекуррентной последовательности максимальной длины.

Таким образом, возможные значения информационных векторов в этих двух случаях должны лежать в диапазоне от 1 до (2^k–1) = 31, то есть (00001)–(11111).

Вариант, когда информация содержится в показателе степени j вектора, напротив, допускает нулевое значение информационного вектора, но вынуждает игнорировать значение (2^k–1) = 31. Это связано с тем, что каждое поле GF(2^5) является циклически замкнутой группой, в которой выполняется равенство $\eta^{31} = \eta^0 = 1$. Поэтому данный вариант позволяет задать информацию на диапазоне от 0 до (2^k – 2) = 30, то есть (00000)–(11110).

Используя этот подход, необходимо учесть, что появление нулевого значения в результате обработки последовательности Голда на приеме следует расценивать как отсутствие информации в канале, так как не существует степени для η, которая бы привела к появлению нулевого вектора поля.

Рассмотрим пример с передачей информации по всем шести каналам, остановившись на варианте представления информации в разрядах вектора (таблица 2).

ТАБЛИЦА 2. Организация передачи данных по шести каналам

TABLE 2. Organization of Data Transmission Over Six Channels

Номер канала i	Информация (элемент поля η^j)	Адресная последовательность $\{S\}_i$
1	(00011) = η^{21}	(11010100001001011001111100011 01)
2	(11000) = η^{20}	(00001100100111110111000101011 01)
3	(10010) = η^5	(10101110110001111100110100100 00)
4	(00110) = η^{14}	(11010100011101111100100110000 10)
5	(11110) = η^8	(11100001101010010001011111011 00)
6	(11111) = η^{10}	(01010110000111001101111101000 10)

Информационные векторы (см. таблицу 2) сопоставляются элементам η^j своих полей GF(2^5), а *M*-последовательности $\{S\}_i$, выступающие в качестве адресных, могут быть получены путем сдвига на j разрядов соответствующих канонических $\{S\}_i$ из таблицы 1.

Последовательность Голда, сформированная по принципу (7) для шести *M*-последовательностей, будет иметь вид:

$$\{\Gamma\} = (00010101101111110010001001111 00). \quad (19)$$

Целью обработки последовательности (19) на приеме является определение всех элементов η^j, которые являются начальными фазами входящих в ее состав адресных *M*-последовательностей.

Первым шагом на пути к этому должно стать построение общего характеристического многочлена, который является произведением (20) всех шести минимальных полиномов [7]. Далее определяется производная для (20), которая будет иметь вид (21) из [7].

$$P(x) = P_1(x)P_2(x)P_3(x)P_4(x)P_5(x)P_6(x) = x^{30} + x^{29} + x^{28} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + \\ + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + \\ + x^4 + x^3 + x^2 + x + 1. \quad (20)$$

$$P'(x) = x^{28} + x^{26} + x^{24} + x^{22} + x^{20} + x^{18} + x^{16} + x^{14} + x^{12} + x^{10} + x^8 + x^6 + x^4 + x^2 + 1. \quad (21)$$

Полученные многочлены (20) и (21) при помощи выражения (14) позволяют определить для всех шести каналов, соответствующих своим полям, полные наборы из $m = 6k = 30$ базисных коэффициентов (таблица 3).

ТАБЛИЦА 3. Базисные коэффициенты для последовательности Голда

TABLE 3. Basic Coefficients for the Gold Sequence

Базисные коэффициенты	Каналы					
	1	2	3	4	5	6
	$P_1(x)$	$P_2(x)$	$P_3(x)$	$P_4(x)$	$P_5(x)$	$P_6(x)$
λ_1	η^{18}	η^{20}	η^{14}	η^{12}	η^{13}	η^{19}
λ_2	η^{4}	η^{8}	η^{27}	η^{23}	η^{25}	η^{6}
λ_3	η^{27}	η^{24}	η^{3}	η^{6}	η^{21}	η^{9}
λ_4	η^{7}	η^{15}	η^{22}	η^{14}	η^{18}	η^{11}
λ_5	η^{29}	η^{4}	η^{30}	η^{24}	η^{3}	η^{25}
λ_6	η^{22}	η^{16}	η^{5}	η^{11}	η^{10}	η^{17}
λ_7	η^{16}	η^{23}	η^{10}	η^{3}	η^{30}	η^{27}
λ_8	η^{13}	η^{29}	η^{12}	η^{27}	η^{4}	η^{21}
λ_9	η^{8}	η^{25}	η^{16}	η^{30}	η^{17}	η^{7}
λ_{10}	η^{26}	η^{7}	η^{28}	η^{16}	η^{5}	η^{18}
λ_{11}	η^{9}	η^{2}	η^{13}	η^{20}	η^{29}	η^{24}
λ_{12}	η^{12}	1	η^{9}	η^{21}	η^{19}	η^{2}
λ_{13}	η^{2}	η^{5}	η^{18}	η^{15}	η^{20}	1
λ_{14}	1	η^{14}	η^{19}	η^{5}	η^{28}	η^{22}
λ_{15}	η^{10}	η^{11}	η^{8}	η^{7}	η^{23}	η^{26}
λ_{16}	η^{25}	η^{26}	η^{23}	η^{22}	η^{7}	η^{10}
λ_{17}	η^{14}	η^{28}	η^{2}	η^{19}	η^{11}	η^{5}
λ_{18}	η^{15}	η^{18}	1	η^{28}	η^{2}	η^{13}
λ_{19}	η^{24}	η^{12}	η^{21}	η^{2}	1	η^{14}
λ_{20}	η^{20}	η^{13}	η^{24}	1	η^{9}	η^{4}
λ_{21}	η^{5}	η^{17}	η^{7}	η^{26}	η^{15}	η^{28}
λ_{22}	η^{17}	η^{3}	η^{25}	η^{8}	η^{26}	η^{16}
λ_{23}	η^{21}	η^{6}	η^{20}	η^{4}	η^{12}	η^{29}
λ_{24}	η^{23}	η^{30}	η^{17}	η^{10}	η^{6}	η^{3}
λ_{25}	η^{28}	η^{22}	η^{11}	η^{17}	η^{16}	η^{23}
λ_{26}	η^{3}	η^{9}	η^{4}	η^{29}	η^{8}	η^{30}
λ_{27}	η^{11}	η^{19}	η^{26}	η^{18}	η^{22}	η^{15}
λ_{28}	η^{30}	η^{27}	η^{6}	η^{9}	η^{24}	η^{12}
λ_{29}	η^{6}	η^{10}	η^{29}	η^{25}	η^{27}	η^{8}
λ_{30}	η^{19}	η^{21}	η^{15}	η^{13}	η^{14}	η^{20}

Теперь, используя формулу (13), нетрудно вычислить элементы поля, соответствующие текущим фазам M-последовательностей, составляющих последовательность (19). Произведем разложение начального m-элементного участка (19) на базисные коэффициенты, что, в данном случае, равнозначно вычислению суммы следующих базисных коэффициентов из таблицы 3: λ_4, λ_6, λ_8, λ_9, λ_{11}, λ_{12}, λ_{13}, λ_{14}, λ_{15}, λ_{16}, λ_{19}, λ_{23}, λ_{26}, λ_{27}, λ_{28}, λ_{29}.

Таким образом, выделим информацию в каждом из шести каналов:

Канал 1: $\eta^7 + \eta^{22} + \eta^{13} + \eta^8 + \eta^9 + \eta^{12} + \eta^2 + 1 + \eta^{10} + \eta^{25} + \eta^{24} + \eta^{21} + \eta^3 + \eta^{11} + \eta^{30} + \eta^6 = \eta^{21}$,
$\eta \in \mathrm{GF}(2^5)$, $P_1(x) = x^5 + x^2 + 1$;

Канал 2: $\eta^{15} + \eta^{16} + \eta^{29} + \eta^{25} + \eta^2 + 1 + \eta^5 + \eta^{14} + \eta^{15} + \eta^{16} + \eta^{29} + \eta^{25} + \eta^2 + 1 + \eta^5 + \eta^{14} + \eta^{11} + \eta^{26} + \eta^{12} + \eta^6 + \eta^9 + \eta^{19} + \eta^{27} + \eta^{10} = \eta^{20}$,
$\eta \in \mathrm{GF}(2^5)$, $P_2(x) = x^5 + x^4 + x^3 + x^2 + 1$;

Канал 3: $\eta^{22} + \eta^5 + \eta^{12} + \eta^{16} + \eta^{13} + \eta^9 + \eta^{18} + \eta^{19} + \eta^8 + \eta^{23} + \eta^{21} + \eta^{20} + \eta^4 + \eta^{26} + \eta^6 + \eta^{29} = \eta^5$,
$\eta \in \mathrm{GF}(2^5)$, $P_3(x) = x^5 + x^3 + 1$;

Канал 4: $\eta^{14} + \eta^{11} + \eta^{27} + \eta^{30} + \eta^{20} + \eta^{21} + \eta^{15} + \eta^5 + \eta^7 + \eta^{22} + \eta^2 + \eta^4 + \eta^{29} + \eta^{18} + \eta^9 + \eta^{25} = \eta^{14}$,
$\eta \in \mathrm{GF}(2^5)$, $P_4(x) = x^5 + x^3 + x^2 + x + 1$;

Канал 5: $\eta^{18} + \eta^{10} + \eta^4 + \eta^{17} + \eta^{29} + \eta^{19} + \eta^{20} + \eta^{28} + \eta^{23} + \eta^7 + 1 + \eta^{12} + \eta^8 + \eta^{22} + \eta^{24} + \eta^{27} = \eta^8$,
$\eta \in \mathrm{GF}(2^5)$, $P_5(x) = x^5 + x^4 + x^3 + x + 1$;

Канал 6: $\eta^{11} + \eta^{17} + \eta^{21} + \eta^7 + \eta^{24} + \eta^2 + 1 + \eta^{22} + \eta^{26} + \eta^{10} + \eta^{14} + \eta^{29} + \eta^{30} + \eta^{15} + \eta^{12} + \eta^8 = \eta^{10}$,
$\eta \in \mathrm{GF}(2^5)$, $P_6(x) = x^5 + x^4 + x^2 + x + 1$.

Обработка последовательности (19) базисными коэффициентами, как показано в примере, позволила однозначно определить информационные векторы, соответствующие начальным фазам (см. таблицу 2). Таким образом, одна двоичная последовательность Голда (19) обеспечила одновременную передачу пяти информационных разрядов по каждому из шести независимых каналов.

Приведем второй пример, где в один момент времени будет задействована только половина всех каналов. То есть три канала являются активными, а другие три не передают информации. В таком случае общая последовательность Голда строится на основе суммы по mod 2 трех M-последовательностей (см. таблицу 1) с учетом их начальных фаз, которые будут определять саму информацию. Отсутствие информации в неиспользуемых каналах обозначим векторами (00000) = NULL (таблица 4, где i – номер канала, Q – элемент поля η^j, R – адресная последовательность $\{S\}_i$).

ТАБЛИЦА 4. Организация передачи данных по трем каналам

TABLE 4. Organization of Data Transmission Over Three Channels

i	*Q*	*R*
1	(00011) = η^{15}	(00110111010100001001011001111110)
2	(11000) = η^{7}	(11000101011010000110010011111101)
3	(10010) = η^{24}	(01101001000010101110110001111110)
4	(00000) = NULL	–
5	(00000) = NULL	–
6	(00000) = NULL	–

Три адресные комбинации, соответствующие первым трем активным каналам, образуют последовательность Голда:

$$\{\Gamma\} = (1001101100110010000111101111101). \quad (22)$$

Как и в предыдущем примере, целью здесь является определение всех элементов η^j, которые являются начальными фазами входящих в состав (22) адресных *M*-последовательностей или определение факта их отсутствия.

Используя уже вычисленные ранее базисные коэффициенты (см. таблицу 3), разложим начальный *m*-элементный участок (22). Для этого достаточно определить сумму следующего набора базисных коэффициентов: λ_1, λ_4, λ_5, λ_7, λ_8, λ_{11}, λ_{12}, λ_{15}, λ_{20}, λ_{21}, λ_{22}, λ_{23}, λ_{25}, λ_{26}, λ_{27}, λ_{28}, λ_{29}.

Определим информацию во всех каналах:

Канал 1: $\eta^{18} + \eta^{7} + \eta^{29} + \eta^{16} + \eta^{13} + \eta^{9} + \eta^{12} + \eta^{10} + \eta^{20} + \eta^{5} + \eta^{17} + \eta^{21} + \eta^{28} + \eta^{3} + \eta^{11} + \eta^{30} + \eta^{6} = \eta^{15}$,
$\eta \in \mathrm{GF}(2^5)$, $P_1(x) = x^5 + x^2 + 1$;

Канал 2: $\eta^{20} + \eta^{15} + \eta^{4} + \eta^{23} + \eta^{29} + \eta^{2} + 1 + \eta^{11} + \eta^{13} + \eta^{17} + \eta^{3} + \eta^{6} + \eta^{22} + \eta^{9} + \eta^{19} + \eta^{27} + \eta^{10} = \eta^{7}$,
$\eta \in \mathrm{GF}(2^5)$, $P_2(x) = x^5 + x^4 + x^3 + x^2 + 1$;

Канал 3: $\eta^{14} + \eta^{22} + \eta^{30} + \eta^{10} + \eta^{12} + \eta^{13} + \eta^{9} + \eta^{8} + \eta^{24} + \eta^{7} + \eta^{25} + \eta^{20} + \eta^{11} + \eta^{4} + \eta^{26} + \eta^{6} + \eta^{29} = \eta^{24}$,
$\eta \in \mathrm{GF}(2^5)$, $P_3(x) = x^5 + x^3 + 1$;

Канал 4: $\eta^{12} + \eta^{14} + \eta^{24} + \eta^{3} + \eta^{27} + \eta^{20} + \eta^{21} + \eta^{7} + 1 + \eta^{26} + \eta^{8} + \eta^{4} + \eta^{17} + \eta^{29} + \eta^{18} + \eta^{9} + \eta^{25} = \mathrm{NULL}$,
$\eta \in \mathrm{GF}(2^5)$, $P_4(x) = x^5 + x^3 + x^2 + x + 1$;

Канал 5: $\eta^{13} + \eta^{18} + \eta^{3} + \eta^{30} + \eta^{4} + \eta^{29} + \eta^{19} + \eta^{23} + \eta^{9} + \eta^{15} + \eta^{26} + \eta^{12} + \eta^{16} + \eta^{8} + \eta^{22} + \eta^{24} + \eta^{27} = \mathrm{NULL}$,
$\eta \in \mathrm{GF}(2^5)$, $P_5(x) = x^5 + x^4 + x^3 + x + 1$;

Канал 6: $\eta^{19} + \eta^{11} + \eta^{25} + \eta^{27} + \eta^{21} + \eta^{24} + \eta^{2} + \eta^{26} + \eta^{4} + \eta^{28} + \eta^{16} + \eta^{29} + \eta^{23} + \eta^{30} + \eta^{15} + \eta^{12} + \eta^{8} = \mathrm{NULL}$,
$\eta \in \mathrm{GF}(2^5)$, $P_6(x) = x^5 + x^4 + x^2 + x + 1$.

Как видно из обработки *m*-элементного участка, информация присутствует в первых трех каналах, а в остальных трех регистрируется ее отсутствие. При этом вычисленные значения начальных фаз для первых трех каналов являются абсолютно верными и совпадают со значениями из таблицы 4.

Множественный доступ на основе двухэтапного расширения спектра

Пускай имеется некоторое число узлов *N*, которые являются равнозначными участниками обмена данными в сети связи. Каждый из них в любой момент времени может осуществить одновременную передачу *k* индивидуальных бит информации остальным узлам. При этом широкополосный сигнал, передаваемый в открытом канале связи, не должен выдавать информацию о связи отправителя с получателем.

Учитывая рассмотренные выше методы кодового уплотнения, подобная схема может быть реализована в два этапа, которые призваны обеспечить первичное и вторичное расширение спектра исходного сигнала методом DSSS (рисунок 3).

На первом этапе *k* бит информации, предназначенные для каждого узла, расширяются до $n = 2^k - 1$ разрядов. При этом для каждого узла из множества *N* используется *M*-последовательность, построенная на основании своего минимального многочлена (таблица 5).

ТАБЛИЦА 5. Матрица соответствия между отправителями и получателями

TABLE 5. Correspondence Matrix between Senders and Recipients

Номера узлов		Отправители (адресные последовательности)						
		1	2	3	4	5	…	*N*
Получатели	1		$P_1(x)$	$P_2(x)$	$P_3(x)$	$P_4(x)$	…	$P_N(x)$
	2	$P_N(x)$		$P_1(x)$	$P_2(x)$	$P_3(x)$	…	$P_{N-1}(x)$
	3	$P_{N-1}(x)$	$P_N(x)$		$P_1(x)$	$P_2(x)$	…	$P_{N-2}(x)$
	4	$P_{N-2}(x)$	$P_{N-1}(x)$	$P_N(x)$		$P_1(x)$	…	$P_{N-3}(x)$
	5	$P_{N-3}(x)$	$P_{N-2}(x)$	$P_{N-1}(x)$	$P_N(x)$		…	$P_{N-4}(x)$
	…	…	…	…	…	…		…
	N	$P_1(x)$	$P_2(x)$	$P_3(x)$	$P_4(x)$	$P_5(x)$	…	

Затем производится формирование эквивалентного кода Голда путем суммирования по mod 2 всех построенных ранее *M*-последовательностей.

На втором этапе каждый из *n* разрядов эквивалентного кода Голда умножается на адресную последовательность длины $L = 2^l - 1$ в соответствии с принципом (4). Полученные в результате этого преобразования прямые и инверсные адресные комбинации модулируются QPSK и передаются в общий канал связи, где в силу своей ортогональности не будут оказывать влияния на адресные комбинации других узлов.

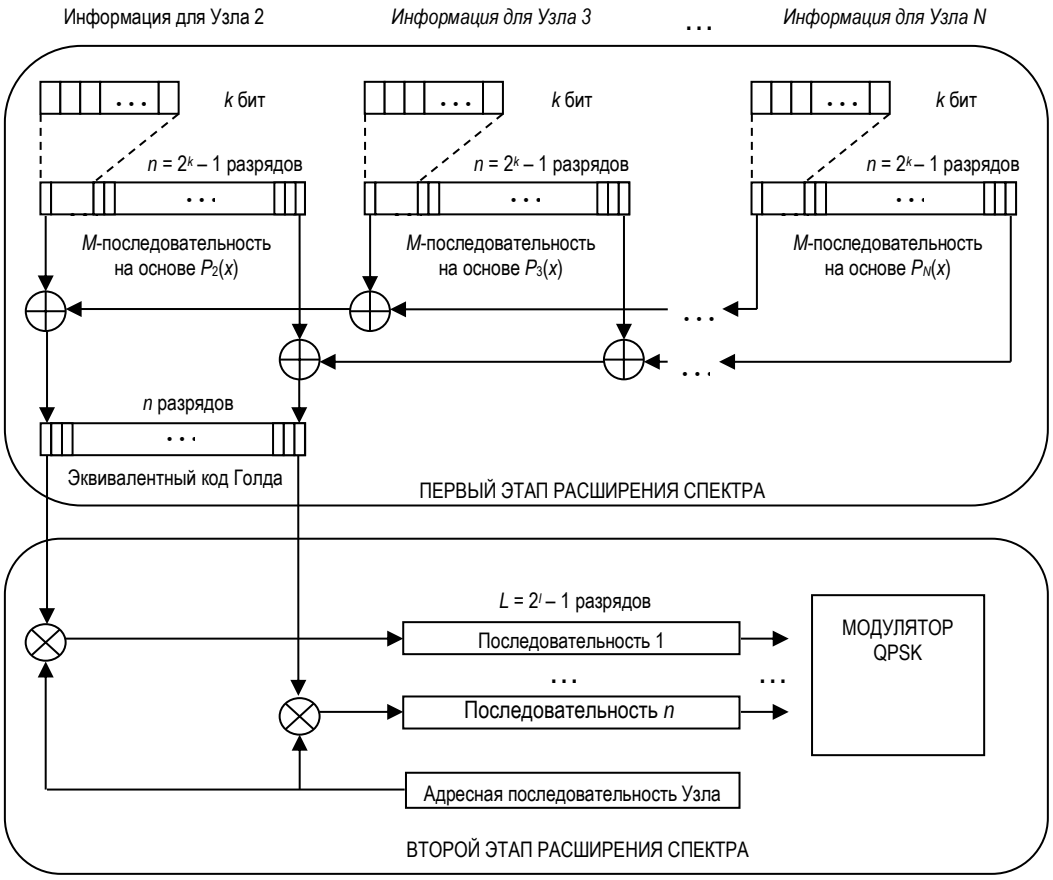

Рис. 3. Обмен данными Узла 1 с остальными узлами

Fig. 3. Node 1 Data Exchange with Other Nodes

На приеме каждый узел выделяет адресные последовательности, полученные от всех узлов. После этого, используя матрицу соответствия (см. таблицу 5), узел-получатель определяет переданные индивидуально для него *M*-последовательности, входящие в состав принятого им кода Голда. Начальные фазы этих *M*-последовательностей (первые k элементов или порождающий элемент поля Галуа) будут соответствовать информационным битам, переданным соответствующими узлами-отправителями.

Анонимность внутри сети, когда отдельно взятый узел не знает, какая информация была адресована остальным узлам, реализуется путем исключения из его матрицы соответствия (см. таблицу 5) лишних строк и столбцов. Так, узлу, производящему передачу данных, необходим только столбец с его номером, а узлу, принимающему данные, только его строка.

Число строк и столбцов матрицы соответствия (см. таблицу 5) определяется количеством узлов сети N, между которыми осуществляется параллельная передача данных. Данная характеристика задает требования к длине последовательностей, применяемых на первом и втором этапах расширения спектра сигнала:

$$\begin{cases} (N-1) \le \left[\dfrac{\phi(2^k-1)}{k}\right] \\ N \le 2^{l-1} \end{cases} \qquad (23)$$

Верхнее условие (23) показывает, что число связей между каждым из N узлов сети со всеми остальными узлами, определяемое как $(N - 1)$, не должно превышать количества используемых системой минимальных многочленов на первом этапе расширения спектра сигнала. Зависимость максимально допустимого числа N узлов сети от параметра k приведена ниже (таблица 6).

ТАБЛИЦА 6. Максимально допустимое число узлов сети

TABLE 6. Maximum Allowed Number of Network Nodes

k	3	4	5	6	7	8	9	10	11	12
N	3	3	7	7	19	17	49	61	177	145

Второе условие целиком и полностью применимо к методике построения ортогональных последовательностей, базирующейся на принципе (3). Вместе с тем, ничто не мешает использовать на втором этапе расширения спектра сигнала альтернативные наборы адресных последовательностей, длина которых обеспечит уникальность узлов, передающих информацию.

Рассмотрим пример сети, где на первом этапе расширения спектра для информационного блока, состоящего из $k = 5$ бит, планируется использовать сформированный ранее набор минимальных многочленов степени k над полями GF(2^5). Количество таких многочленов составляет $V = 6$ (см. таблицу 1). Таким образом, число связей между каждым отдельно взятым узлом и всеми остальными узлами сети не должно превышать $N - 1 = 6$.

Очевидно, такая сеть может включать в себя максимум $N = 7$ узлов, для каждого из которых в дальнейшем должна быть определена своя уникальная адресная последовательность A_i, где $i = 1, 2, \ldots, 7$ (рисунок 4). Общий вид матрицы соответствия для сети представлена в таблице 7.

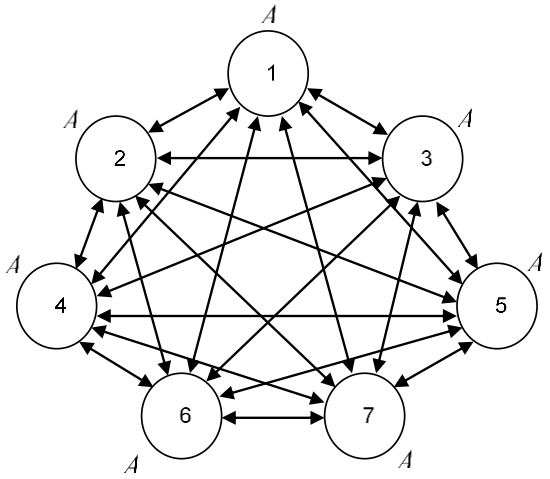

Рис. 4. Сеть параллельной передачи данных, состоящая из $N = 7$ узлов

Fig. 4. Parallel Data Transmission Network Consisting of N = 7 Nodes

В качестве адресных последовательностей на втором этапе расширения спектра сигнала, как вариант, могут быть использованы классические функции Уолша длины 8 или комбинации периода $L = 2^4 - 1 = 15$, построенные ранее из линейных рекуррентных последовательностей максимальной длины на основе многочлена $P(x) = x^4 + x + 1$ над полем GF(2^4).

ТАБЛИЦА 7. Матрица соответствия для сети из семи узлов

TABLE 7. Matching Matrix for a Network of Seven Nodes

Номера узлов		Отправители						
		1	2	3	4	5	6	7
Получатели	1		$P_1(x)$	$P_2(x)$	$P_3(x)$	$P_4(x)$	$P_5(x)$	$P_6(x)$
	2	$P_6(x)$		$P_1(x)$	$P_2(x)$	$P_3(x)$	$P_4(x)$	$P_5(x)$
	3	$P_5(x)$	$P_6(x)$		$P_1(x)$	$P_2(x)$	$P_3(x)$	$P_4(x)$
	4	$P_4(x)$	$P_5(x)$	$P_6(x)$		$P_1(x)$	$P_2(x)$	$P_3(x)$
	5	$P_3(x)$	$P_4(x)$	$P_5(x)$	$P_6(x)$		$P_1(x)$	$P_2(x)$
	6	$P_2(x)$	$P_3(x)$	$P_4(x)$	$P_5(x)$	$P_6(x)$		$P_1(x)$
	7	$P_1(x)$	$P_2(x)$	$P_3(x)$	$P_4(x)$	$P_5(x)$	$P_6(x)$	

Таким образом, на первом этапе расширения спектра любой, передающий информацию узел-отправитель, определяет, какие узлы-получатели должны будут принять каждый свои $k = 5$ информационных бит. Для этого столбец матрицы соответствия (см. таблицу 7) задает шесть M-последовательностей с соответствующими начальными фазами на основе минимальных многочленов. Эти M-последовательности будут в последствии просуммированы по mod 2 и упакованы в код Голда.

Второй этап расширения спектра произведет замену каждого разряда последовательности Голда на прямую или инверсную адресную последовательность с последующей модуляцией QPSK в режиме передачи одного разряда. Таким образом, каждый узел должен отправить свои разряды последовательности эквивалентного кода Голда в канал связи, используя последовательный принцип передачи данных или разделение частот. На приемной стороне ортогональная природа адресных последовательностей позволит узлу-получателю определить, от каких узлов-отправителей были получены адресные последовательности, восстановить их коды Голда целиком, а затем, используя строку матрицы соответствия (см. таблицу 7), выделить начальные фазы входящих в их состав M-последовательностей.

Заключение

Данная работа рассматривает технологию двойного расширения спектра сигнала, где на первом этапе задаются адреса получателей, а на втором – адреса отправителей информации. Таким образом, идентификация сторон определяется на физическом уровне, что снимает последующую нагрузку на верхние уровни системы передачи данных.

Несомненным преимуществом данного метода расширения спектра сигнала является анонимность, которая обеспечивается матрицами соответствия, хранимыми на узлах сети. При этом возможна также реализация анонимности узлов между собой путем удаления из этих матриц лишних строк и столбцов, отвечающих за связность других узлов-отправителей с узлами-получателями.

Метод кодового уплотнения на основе эквивалентных кодов Голда, применяемый на первом этапе расширения спектра сигнала, вполне можно считать альтернативой используемым до настоящего времени ортогональным методам. Несмотря на свою квазиортогональную природу, последовательности максимальной длины в данном случае ее не используют, так как вся обработка уплотненного сигнала строится на разложении по двойственному базису поля Галуа.

Еще раз отметим основные особенности неортогонального кодового уплотнения на основе последовательностей Голда.

Во-первых, в отличие от классических, эквивалентные последовательности Голда могут включать в себя произвольное число *M*-последовательностей от разных характеристических полиномов. В приведенных примерах таких рекуррентных последовательностей было шесть.

Во-вторых, последовательности максимальной длины формируют общий сигнал не на основе линейной суммы *M*-последовательностей, а по mod 2. Полученный при этом код Голда будет иметь единичную максимальную амплитуду сигнала, что в дальнейшем позволит применить к нему фазовый тип модуляции.

В-третьих, отсутствует требование к ортогональности адресных последовательностей, входящих в состав кода Голда, так как не планируется вычисление их скалярного произведения с ним.

В-четвертых, в качестве недостатка рассмотренного метода кодового уплотнения следует отметить исключение нулевого или единичного информационного вектора из адресного пространства, в зависимости от способа представления информации.

Также необходимо учесть ошибки, которые могут возникнуть на приеме после выделения адресных последовательностей. Очевидно, что для их исправления можно было бы использовать некоторый помехоустойчивый код.

Список источников

1. Бабков В.Ю., Никитин А.Н., Осенний К.Н., Сиверс М.А. Системы связи с кодовым разделением каналов. СПб.: ТРМАДА, 2003. 239 с.
2. Бобровский В.И. Многопользовательское детектирование. Ульяновск: Вектор-С, 2007. 346 с.
3. Бобровский В.И. Фрактальные алгоритмы многопользовательского детектирования «плотных» ансамблей сигналов // Техника средств связи. 2019. № 4(148). С. 15–28. EDN:YFHTZY
4. Шахнович И.В. Современные технологии беспроводной связи. М.: Техносфера, 2006. 288 с. EDN:QMPRPT
5. Hajar A., Hamamreh J.M., Abewa M., Belallou Y. A Spectrally Efficient OFDM-Based Modulation Scheme for Future Wireless Systems // Proceedings of Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT, Istanbul, Turkey, 24–26 April 2019). IEEE, 2019. DOI:10.1109/EBBT.2019.8742049
6. Du Y., Liu J., Chen Y. Performance Analysis of Nonlinear SFBC OFDM Systems Over TWDP Fading Channel // IEEE Access. 2019. Vol. 7. PP. 101981–101991. DOI:10.1109/ACCESS.2019.2927753
7. Кукунин Д.С., Когновицкий О.С., Березкин А.А., Киричек Р.В. Перспективы использования рекуррентных последовательностей в современной телекоммуникационной среде. СПб.: СПбГУТ, 2023. 289 с.
8. Когновицкий О.С. Широкополосные сигналы данных с расширением спектра прямой последовательностью и их характеристика // Труды учебных заведений связи. 2016. Т. 2. № 1. С. 82–89. EDN:XCGQHP
9. Khudhair A.Y., Abd Khalid R.A. Reduction of the Noise Effect to Detect the DSSS Signal using the Artificial Neural Network // Proceedings of the 1st Babylon International Conference on Information Technology and Science (BICITS, Babil, Iraq, 28-29 April 2021). IEEE, 2021. PP. 185–188. DOI:10.1109/BICITS51482.2021.9509880
10. Visan D.A., Jurian M., Lita I., Ionescu L.M., Mazare A.G. Direct Sequence Spread Spectrum Communication Module for Efficient Wireless Sensor Networks // Proceedings of the 11th International Conference on Electronics Computers and Artificial Intelligence (ECAI, Pitesti, Romania, 27–29 June 2019). IEEE, 2019. DOI:10.1109/ECAI46879.2019.9041979
11. Dmitriyev E.M., Rogozhnikov E.V., Movchan A.K., Mukhamadiev S.M., Krukov Y.V., Duplishcheva N.V. Spread spectrum technology research and its application in power line communication systems // T-Comm. 2020. Vol. 14. Iss. 10. PP. 45–52. DOI:10.36724/2072-8735-2020-14-10-45-52. EDN:VZDBDQ
12. Qiu Z., Peng H., Li T. A Blind Despreading and Demodulation Method for QPSK-DSSS Signal With Unknown Carrier Offset Based on Matrix Subspace Analysis // IEEE Access. 2019. Vol. 7. PP. 125700–125710. DOI:10.1109/ACCESS.2019.2938785
13. Варакин Л.Е. Системы связи с шумоподобными сигналами. М.: Радио и связь, 1985. 384 с.
14. Деев В.В. Методы модуляции и кодирования в современных системах связи. СПб.: Наука, 2007. 268 с.
15. Прокис Дж. Цифровая связь. Пер. с англ. М.: Радио и связь, 2000. 797 с.
16. Никитин Г.И. Применение функций Уолша в сотовых системах связи с кодовым разделением каналов: учебное пособие. СПб.: ГУАП, 2003. 86 с.
17. Кукунин Д.С., Березкин А.А., Киричек Р.В. Многослойные ортогональные структуры на основе последовательностей максимальной длины // Инфокоммуникационные технологии, 2022. Т. 20. № 2(78). С. 42–50. DOI:10.18469/ikt.2022.20.2.05. EDN:DOLLWE
18. Kukunin D., Berezkin A., Kirichek R. Asynchronous Address System Using Code Division Based on Maximum Length Sequences // Proceedings of International Conference on Information, Control, and Communication Technologies (ICCT, Astrakhan, Russian Federation, 03–07 October 2022). IEEE, 2022. DOI:10.1109/ICCT56057.2022.9976772
19. Кукунин Д.С., Березкин А.А., Киричек Р.В., Елисеева К.А. Асинхронная передача данных с использованием многослойных ортогональных структур в системах с кодовым разделением каналов // Электросвязь. 2023. № 1. С. 26–35. DOI:10.34832/ELSV2023.38.1.003. EDN:HNTXND
20. Когновицкий О.С. Двойственный базис и его применение в телекоммуникациях. СПб.: Линк, 2009.

References

1. Babkov V.Yu., Nikitin A.N., Osenniy K.N., Sievers M.A. *Code Division Communication Systems*. St Petersburg: TPMADA Publ.; 2003. 239 p. (in Russ.)
2. Bobrovsky V. N.I. *Multi-user detection*. Ulyanovsk: Vector-C, 2007. 346 p. (in Russ.)
3. Bobrovsky V.I. Fractal algorithms for multiple user detectoring of “dense” signal assemblies. *Means of communication equipment*. 2019;4(148):15–28. (in Russ.) EDN:YFHTZY).
4. Shakhnovich I.V. *Modern Wireless Communication Technology*. Moscow: Tekhnosfera Publ.; 2006. 288 c. p. (in Russ.) EDN:QMPRPT
5. Hajar A., Hamamreh J.M., Abewa M., Belallou Y. A Spectrally Efficient OFDM-Based Modulation Scheme for Future Wireless Systems. *Proceedings of Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science, EBBT, 24–26 April 2019, Istanbul, Turkey*. IEEE; 2019. DOI:10.1109/EBBT.2019.8742049
6. Du Y., Liu J., Chen Y. Performance Analysis of Nonlinear SFBC OFDM Systems Over TWDP Fading Channel. *IEEE Access*. 2019;7:101981–101991. DOI:10.1109/ACCESS.2019.2927753
7. Kukunin D.S., Kognovitsky O.S., Berezkin A.A., Kirichek R.V. *Prospects for the use of recurrent sequences in the modern telecommunications environment*. St Petersburg: The Bonch-Bruevich Saint Petersburg State University of Telecommunications Publ.; 2023. 289 p. (in Russ.)
8. Kognovitzkiy O. Wideband Data Signals with Direct Sequence Spread Spectrum and Their Properties. *Proceedings of Telecommunication Universities*. 2016;2(1):82–89. EDN:XCGQHP
9. Khudhair A.Y., Abd Khalid R.A. Reduction of the Noise Effect to Detect the DSSS Signal using the Artificial Neural Network. *Proceedings of the 1st Babylon International Conference on Information Technology and Science, BICITS, 28–29 April 2021, Babil, Iraq.* IEEE; 2021. p.185–188. DOI:10.1109/BICITS51482.2021.9509880
10. Visan D.A., Jurian M., Lita I., Ionescu L.M., Mazare A.G. Direct Sequence Spread Spectrum Communication Module for Efficient Wireless Sensor Networks. *Proceedings of the 11th International Conference on Electronics Computers and Artificial Intelligence, ECAI, 27–29 June 2019, Pitesti, Romania.* IEEE; 2019. DOI:10.1109/ECAI46879.2019.9041979
11. Dmitriyev E.M., Rogozhnikov E.V., Movchan A.K., Mukhamadiev S.M., Krukov Y.V., Duplishcheva N.V. Spread spectrum technology research and its application in power line communication systems. *T-Comm*. 2020;14(10):45–52. DOI:10.36724/2072-8735-2020-14-10-45-52. EDN:VZDBDQ
12. Qiu Z., Peng H., Li T. A Blind Despreading and Demodulation Method for QPSK-DSSS Signal With Unknown Carrier Offset Based on Matrix Subspace Analysis. *IEEE Access*. 2019;7:125700–125710. DOI:10.1109/ACCESS.2019.2938785
13. Varakin L.E. *Communication Systems with Noise-Like Signals*. Moscow: Radio i svyaz' Publ.; 1985. 384 p. (in Russ.)
14. Deev V.V. *Modulation and Coding Methods in Modern Communication Systems. St Petersburg*: Nauka Publ.; 2007. 268 p. (in Russ.)
15. Proakis J. Digital Communication. Translated from English. Moscow: Radio and Communications Publ.; 2000. 797 p. (in Russ.)
16. Nikitin G.I. *Application of Walsh Functions in Cellular Communication Systems with Code Division of Channels*. St Petersburg: Saint-Petersburg State University of Aerospace Instrumentation Publ.; 2003. 86 p. (in Russ.)
17. Kukunin D.S., Berezkin A.A., Kirichek R.V. Multilayer Orthogonal Structures Based on Maximum Length Sequences. *Infokommunikacionnye Texnologii.* 2022;20(2-78):42–50. (in Russ.) DOI:10.18469/ikt.2022.20.2.05. EDN:DOLLWE
18. Kukunin D., Berezkin A., Kirichek R. Asynchronous Address System Using Code Division Based on Maximum Length Sequences. *Proceedings of International Conference on Information, Control, and Communication Technologies, ICCT, 03–07 October 2022, Astrakhan, Russian Federation*. IEEE; 2022. DOI:10.1109/ICCT56057.2022.9976772
19. Kukunin D.S., Berezkin A.A., Kirichek R.V., Eliseeva K.A. Asynchronous data transfer using multilayer orthogonal structures in CDMA systems. *Elektrosvyaz*. 2023;1:26–35. (in Russ.) DOI:10.34832/ELSV2023.38.1.003. EDN:HNTXND
20. Kognovitsky O.S. *Dual basis and its application in telecommunications*. St Petersburg: Link Publ.; 2009. (in Russ.)

Статья поступила в редакцию 04.04.2024; одобрена после рецензирования 11.06.2024; принята к публикации 12.06.2024.
The article was submitted 04.04.2024; approved after reviewing 11.06.2024; accepted for publication 12.06.2024.

Информация об авторе:

КУКУНИН Дмитрий Сергеевич
кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0000-0002-2674-5217

Автор сообщает об отсутствии конфликтов интересов.
The author declares no conflicts of interests.