DOI 10.37882/2223–2966.2021.11.31

# АЛГОРИТМ СКРЫТНОГО ИНФОРМАЦИОННОГО ОБМЕНА В СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ С КОДОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ НА ОСНОВЕ ХАОТИЧЕСКОГО ПРИМЕНЕНИЯ ОРТОГОНАЛЬНЫХ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ[1]

## ALGORITHM OF COVERT INFORMATION EXCHANGE IN INFORMATION TRANSMISSION SYSTEMS WITH CODE DIVISION MULTIPLE ACCESS BASED ON CHAOTIC APPLICATION OF ORTHOGONAL CODE SEQUENCES

***A. Studenikin A.V.***

*Summary.* An algorithm of covert information exchange in information transmission systems with code channel separation based on the chaotic use of multiphase orthogonal code sequences ensembles is presented. The algorithm is implemented on the basis of seven stages and allows to increase the security of information exchange based on structural secrecy. The results of the comparison show that the use of an increased number of ensembles of multiphase orthogonal code sequences represented by the eigenvectors of Hermitian matrices increases the structural secrecy of information transmission systems with code channel separation.

*Keywords:* cognitive radio, information transmission systems with code division multiple access, ensembles of multiphase orthogonal code sequences, eigenvectors of Hermitian matrices, security, structural secrecy.

***Студеникин Андрей Владимирович***
*Инженер-исследователь, ФГАОУ ВО*
*«Северо-Кавказский федеральный университет»*
*(г. Ставрополь)*
*studentstavropol@mail.ru*

*Аннотация.* Представлен алгоритм скрытного информационного обмена в системах передачи информации с кодовым разделением каналов на основе хаотического применения ансамблей многофазных ортогональных кодовых последовательностей. Алгоритм реализуется на основе семи основных этапов и позволяет повысить защищённость информационного обмена на основе структурной скрытности. Результаты сравнения показывают, что использование увеличенного количества ансамблей многофазных ортогональных кодовых последовательностей, представляемых собственными векторами эрмитовых матриц, повышает структурную скрытность систем передачи информации с кодовым разделением каналов.

*Ключевые слова:* когнитивное радио, системы передачи информации с кодовым разделением каналов, ансамбли многофазных ортогональных кодовых последовательностей, собственные векторы эрмитовых матриц, защищённость, структурная скрытность.

## Введение

При создании современных беспроводных радиосетей возникают следующие проблемы, требующие решения: нехватка радиочастотного диапазона (спектра), обеспечение электромагнитной совместимости беспроводных систем, организация эффективного управления сетью и её элементами, обеспечение качественных показателей при передаче информации.

Вариантом решения данных проблем является применение систем когнитивного радио (cognitive radio, CR), которые должны работать, не создавая помех и не требуя защиты от других радиоэлектронных средств [1]. Система когнитивного радио производит мониторинг радиоэфира в режиме реального времени и обнаруживает неиспользуемые участки спектра с целью их возможного задействования для передачи информации. Для реализации возложенных на системы

[1] Исследование выполнено при финансовой поддержке Минобрнауки России (Грант ИБ) в рамках научного проекта № 29/2020

когнитивного радио функций, она, как правило, реализует когнитивный цикл, включающий в себя следующие этапы: мониторинг условий работы, сканирование частотного диапазона, установление соединения и обмен информацией между узлами.

К наиболее приемлемым технологиям физического уровня систем когнитивного радио следующие: модуляция на основе синтезированного банка фильтров FBMC, OFDM с дополнительной фильтрацией (f-OFDM), обобщенное мультиплексирование с частотным разделением (GFDM) и мультиплексирование с частотным разделением и универсальной фильтрацией (UFMC). Вместе с тем к настоящему времени достаточно полно проработан вопрос применения в беспроводных радиосетях технологий радиодоступа на основе кодового разделения каналов (CDMA — Code Division Multiple Access) IS-95, cdmaOne, CDMA2000 и W-CDMA, которая имеет преимущества по сравнению с другими технологиями по помехоустойчивости, эффективности использования радиочастотного спектра, скрытности и другим показателям.

Анализ ряда работ по данной теме показал, что внедрение новых систем когнитивного радио создает новые угрозы безопасности информации, которые появляются в связи с концепцией динамического доступа к спектру, а также потребностями аутентификации элементов системы когнитивного радио [2]. По этой причине решение вопросов защиты информации в системах когнитивного радио имеет актуальное значение.

Анализ существующих направлений повышения защищенности систем связи (СС) с кодовым разделением каналов (КРК) на основе структурной скрытности позволяет выделить следующие направления решения данной задачи.

Первое направление основано на автоматической смене известных структур ансамблей дискретных ортогональных сигналов (АДОС). Для реализации данного подхода повышения структурной скрытности используют такие ортогональные ансамбли как Уолша, OVSF, Стиффлера, Рида-Мюллера, Джеффи, Велти, D-коды, Адамара, Радемахера, Хаара, коды Голда и др. [3–13].

Второе направление повышения структурной скрытности СС с КРК заключается в использовании в качестве расширяющих нелинейных псевдослучайных последовательностей ПСП [14].

Третье направление повышения защищенности СС с КРК на основе структурной скрытности, заключается в использовании ансамблей дискретных ортогональных последовательностей (АДОП), получаемых на основе векторного синтеза [3, 7–9, 15]. Данный подход к формированию АДОП является линейным и представляет собой расчет программным методом собственных векторов бидиагональной симметрической матрицы.

Четвертое направление основано на использовании функциональных преобразований псевдослучайных аргументов для синтеза и последующего хаотического использования систем дискретных квазиортогональных кодовых последовательностей (СДККП) в системах глобальной спутниковой навигации [16], которое обеспечивает повышение структурной скрытности последних.

Пятое направление основано на использовании последовательностей де Брейна со сменой формы последовательности в процессе передачи сообщения от одного информационного символа к другому для реализации процедуры засекречивания с одновременным повышением уровня скрытности передачи СС с КРК [17].

Не смотря на разнообразие известных подходов повышения защищенности СС с КРК на основе структурной скрытности, они имеют существенные обобщенные недостатки, которые заключаются в следующем:

1. ограниченность количества используемых структур ансамблей (систем) ортогональных и квазиортогональных кодовых последовательностей в требуемом диапазоне размерностей;
2. несовершенство алгоритмов формирования ансамблей ортогональных кодовых последовательностей различных размерностей;
3. наличие у ансамблей ортогональных кодовых последовательностей сигналов с неудовлетворительными корреляционными характеристиками, ограничивающими их практическое использование;
4. использование ансамблей многоуровневых ортогональных кодовых последовательностей сигналов возможно только в каналах связи с низким уровнем помех, которые в технике беспроводной связи практически отсутствуют.

С учетом выявленных недостатков известных подходов повышения защищенности СС с КРК на основе структурной скрытности можно сделать вывод об их ограниченности и необходимости поиска усовершенствованного способа повышения защищенности СС с КРК на основе структурной скрытности.

Целью статьи является повышение защищённости информации в системах связи с кодовым разделением каналов на основе хаотического применения ансамблей многофазных ортогональных кодовых последовательностей.

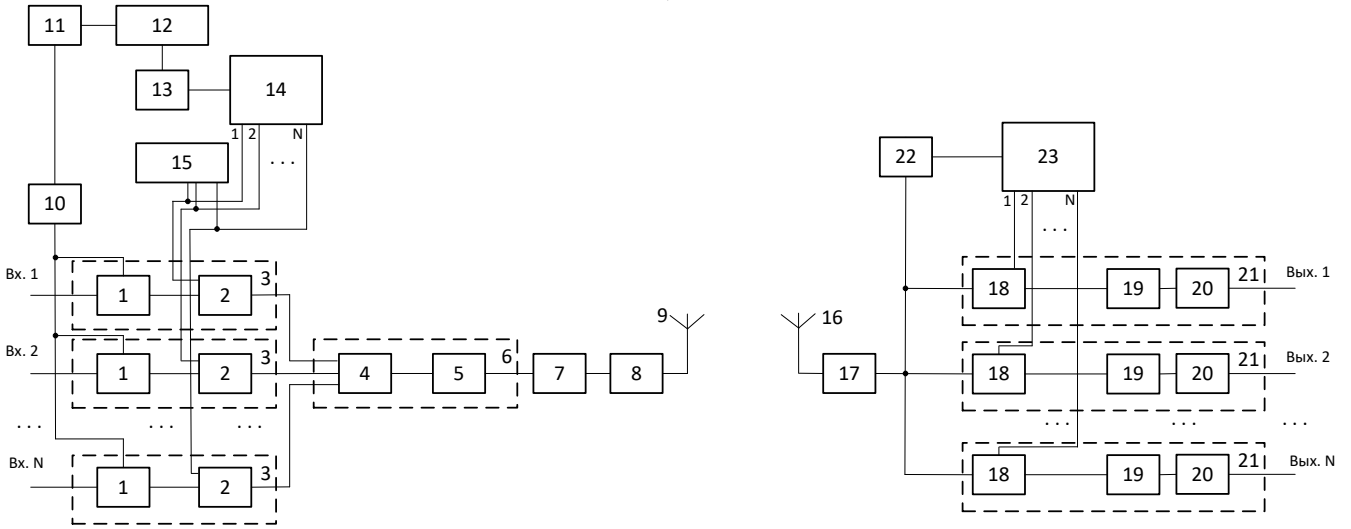


Рис. 1. Структура защищённой системы связи с кодовым разделением каналов

Задачей статьи является разработка алгоритма скрытного информационного обмена в СС с КРК на основе хаотического применения АМОКП.

## Объекты и методы исследования

Анализ работ [6, 18–22] показывает, что наибольший показатель структурной скрытности рассматриваемых систем связи может обеспечить хаотическое применение ансамблей многофазных ортогональных кодовых последовательностей (АМОКП), получаемых на основе векторного синтеза при рассмотрении собственных векторов эрмитовых матриц (ЭМ). В этом случае возможно получение множества АМОКП, имеющего достаточное количество их реализаций для стохастического использования в СС с КРК различных размерностей, обладающих приемлемыми для использования корреляционными характеристиками.

Вопросы разработки универсального формирователя АМОКП и алгоритма его работы рассмотрены в [18]. Достоинствами предложенного подхода является то, что он, во-первых, позволяет на единой алгоритмической основе осуществлять генерацию АМОКП различных размерностей, а, во-вторых, количество генерируемых последовательностей имеет наибольшее значение, по сравнению с известными устройствами и алгоритмами.

По мнению автора, разработку алгоритма скрытного информационного обмена в СС с КРК на основе хаотического применения АМОКП, целесообразно решать на основе описанного в [23, 24] алгоритма и программы синтеза АМОКП, а также представленного в [18] метода их формирования.

Разработаем структуру защищённой СС с КРК и алгоритм скрытного информационного обмена на основе хаотического применения ансамблей многофазных ортогональных кодовых последовательностей. Структура защищённой СС с КРК представлена на рисунке 1.

На рисунке 1 используются следующие обозначения. На передающей стороне: 1 — запоминающие устройства, 2 — модуляторы каналов, 3 — каналы передачи информации, 4 — объединитель входов, 5 — модулятор блока формирования группового сигнала, 6 — блок формирования группового сигнала, 7 — блок фазовой модуляции, 8 — усилитель мощности, 9 –передающая антенна, 10 — блок синхронизации, 11 — генератор случайных чисел, 12 — формирователь эрмитовой матрицы, 14 — блок формирования хаотических ансамблей ортогональных кодовых последовательностей, 15 — запоминающее устройство. На приемной стороне: 16 — приемная антенна, 17 — блок высокочастотной селекции, 18 — блоки корреляционной обработки, 19 — блоки выделения информации, 20 — блоки приема информации, 21 — каналы приема информации, 22 — блок обнаружения сигнала синхронизации, 23 — блок хранения данных.

Алгоритм скрытного информационного обмена в СС с КРК на основе хаотического применения АМОКП на примере рисунка 1 реализуется следующим образом.

1. На первом этапе с помощью вспомогательного синхронизирующего сложного сигнала передающая аппаратура и приемная аппаратура СС с КРК вводится в цикловую фазу.
2. На втором этапе посредством манипуляции вспомогательного сигнала синхронизации на каждый

Таблица 1. Результаты расчетов количества возможных структур уникальных ансамблей последовательностей, полученных различными методами

| Размерность последовательностей, $N$ | Количество уникальных АМОКП | Количество последовательностей де Брейна | ПСХП-1 | ПСХП-2 | ПСХП-3 |
|---|---|---|---|---|---|
| 4 | 287.2 | 1 | 4 | 4 | 1 |
| 8 | $4.595 \cdot 10^3$ | 2 | 10 | 9 | 3 |
| 16 | $1.176 \cdot 10^6$ | 12 | 25 | 18 | 11 |
| 32 | $7.709 \cdot 10^{10}$ | 288 | 57 | 36 | 36 |
| 64 | $3.311 \cdot 10^{20}$ | 34560 | 132 | 73 | 118 |

канал передается служебная информация (единый начальный блок для всех абонентских станций). После выполнения указанной процедуры устанавливается синхронизм между передающей и приемной частью СС с КРК.

3. На третьем этапе начинается одновременная передача всем абонентам цифровой информации, при этом каждому биту информации фиксированного канала ставится в соответствие многофазный сигнал, структура которого зависит от значений диагональных коэффициентов ЭМ, используемых в качестве исходных данных для формирования АМОКП в универсальном формирователе, рассмотренном выше.
4. На четвертом этапе после передачи очередного информационного бита на передающей и приемной стороне производится синхронная смена диагональных коэффициентов ЭМ, поступающих от идентичных генераторов псевдослучайных чисел, расположенных на приемной и передающей стороне, на основе которых происходит расчет АМОКП, описываемых СВ ЭМ. При этом сигнал, используемый на приемной стороне для корреляционной обработки, будет иметь структуру, совпадающую с сигналом, формируемым на передающей стороне, и, следовательно, может быть использован для обработки информационного потока, адресованного получателю цифровой информации.
5. На пятом этапе производится следующая синхронная смена диагональных коэффициентов ЭМ, поступающих от идентичных генераторов псевдослучайных чисел, расположенных на приемной и передающей стороне, на основе которых происходит расчет АМОКП и повторение процесса передачи очередного информационного бита с помощью АМОКП новой структуры.
6. На шестом этапе с целью исключения повтора использования одного и того же АМОКП осуществляется проверка сформированных на предыдущих этапах ансамблей и используемого в данный момент времени. Если в результате сравнения есть отличия между использованными ранее и новым АМОКП, то он разрешается к использованию, в противном случае использование ранее применявшегося АМОКП блокируется. После чего на передающей и приемной стороне производится синхронная смена коэффициентов ЭМ, поступающих от идентичных генераторов псевдослучайных чисел, и повторяется процесс формирования новых АМОКП, предназначенных для передачи последующих информационных символов.
7. На последующих этапах повторяются действия, описанные для 1–6 этапов алгоритма, до тех пор, пока процесс передачи информации не будет завершен, или нарушен по внешним или внутренними причинам. Возобновление работы СС с КРК осуществляется с выполнения действий, предусмотренных первым этапом описанного алгоритма.

## Результаты и обсуждение

Для расчета количества возможных структур ортогональных кодовых последовательностей для матриц четвертого, восьмого, шестнадцатого, тридцать второго и шестьдесят четвертого порядка выведем формулу, в которой будут учитываться следующие параметры:

- $N$ — порядок ЭМ с учетом количества коэффициентов в ЭМ $N–1$;
- значение используемого диапазона градусов — $\Delta\varphi$;
- разрешающая способность детектора — $\Delta$.

Тогда формула для расчета количества возможных структур ортогональных последовательностей $C$ с учетом выше перечисленных параметров примет вид

$$C = 2^{N-1} \cdot \frac{\Delta\varphi}{\Delta} \quad (1)$$

Результаты расчетов количества возможных структур ортогональных последовательностей при изменении значений аргументов на $\Delta = 10^o$ (разрешающей способности фазового детектора) представлены в таблице 1. Также в таблице 1 для сравнения представлены

результаты расчетов количества уникальных последовательностей де Брейна и трех видов псевдослучайных хаотических последовательностей (ПСХП), описанных в [14, 17, 25].

Результаты сравнения показывают, что количество АМОКП, получаемых на основе СВ ЭМ, существенно превышает количество последовательностей, получаемых на основе словарей де Брейна, а также количество псевдослучайных хаотических последовательностей ПСХП-1, ПСХП-2, ПСХП-3. Увеличенное по сравнению с известными количество неповторяющихся структур АМОКП позволяет в течение большего промежутка времени осуществить их стохастическое применение без повторного использования в СС с КРК.

## Заключение

Внедрение новых систем когнитивного радио создает новые угрозы безопасности информации, которые появляются в связи с концепцией динамического доступа к спектру, а также потребностями аутентификации элементов системы когнитивного радио.

Не смотря на разнообразие известных подходов повышения защищенности систем связи СС с КРК на основе структурной скрытности, они имеют существенные недостатки, основным из которых является низкая структурная скрытность. Наибольший показатель структурной скрытности СС с КРК может обеспечить хаотическое применение ансамблей многофазных ортогональных кодовых последовательностей, получаемых на основе векторного синтеза при рассмотрении собственных векторов эрмитовых матриц.

Алгоритм скрытного информационного обмена в СС с КРК на основе хаотического применения АМОКП реализуется на основе семи основных этапов и позволяет повысить защищённость информационного обмена на основе структурной скрытности.

Результаты сравнения показывают, что количество АМОКП, представляемых собственными векторами эрмитовых матриц, существенно превышает количество последовательностей, получаемых на основе словарей де Брейна, а также количество псевдослучайных хаотических последовательностей ПСХП-1, ПСХП-2, ПСХП-3.

ЛИТЕРАТУРА


1. Тихвинский В.О. Динамическое управление радиочастотным ресурсом сетей 5G для различных видов доступа к РЧС // Электросвязь. № 7. 2019. С. 18–22.
2. Ермакова А.В., Бабенко К.А., Мирошникова Н.Е. Текущее состояние и перспективы развития сети 5G // Телекоммуникации и информационные технологии. 2021. Т. 8. № 1. С. 21–28.
3. Варакин Л.Е. Системы связи с шумоподобными сигналами. — М.: Радио и связь, 1985. — 384 с.
4. Варакин Л.Е. Теория сложных сигналов. — М.: Советское радио, 1978. — 199 с.
5. Дядюнов Н.Г., Сенин А.И. Ортогональные и квазиортогональные сигналы. — М.: Связь, 1977. — 224 с.
6. Литюк В.И., Литюк Л.В. Методы цифровой многопроцессорной обработки ансамблей радиосигналов. — М.: Солон-Пресс, 2007. — 592 с.
7. Попенко В.С. Векторный синтез ансамблей ортогональных сигналов. Часть 2. — Ставрополь: МО РФ, 1993. — 131 с.
8. Попенко В.С., Турко С.А. Генератор функций Попенко-Турко // Патент на изобретение SU1753464 A1, опубл. 06.03.1990. — URL: http://elibrary.ru/item.asp?id=23014440 (дата обращения 27.09.2021).
9. Попенко В.С. Оценка ширины спектра дискретных сигналов // Радиотехника. 1996. № 11. С. 57–59.
10. Системы широкополосной радиосвязи: учеб. пособие для студ. вузов. — Одесса: Наука и техника, 2009. — 344 с.
11. Goel S, Chen V Information security risk analysis — a matrix-based approach. Proceedings of the Information Resource Management Association (IRMA) International Conference. — Hershey, USA, 2005. — 9 p.
12. Golomb S. Digital communications with space applications. — Upper Saddle River NJ, Prentice-Hall, 1964. — 210 p.
13. Golomb S. Shift Register Sequences. — San Francisco: Holden-Day, 1967.
14. Сухарев Е.М. и др. Общесистемные вопросы защиты информации. Коллективная монография. Кн. 1. — М.: Радиотехника, 2003. — 296 с.
15. Пашинцев В.П. Малофей О.П., Жук А.П. Развитие теории синтеза и методов формирования ансамблей дискретных сигналов для перспективных систем радиосвязи различных диапазонов радиоволн: Монография — М.: ООО Издательская фирма «ФМЛ», 2010. — 196 с.
16. Орёл Д.В. Моделирование стохастических систем двоичных квазиортогональных кодовых последовательностей на основе метода функциональных преобразований: автореф. дис. … канд. техн. наук: 05.13.18 / Орёл Дмитрий Викторович. — Ставрополь, 2013. — 19 с.
17. Косякин С.И., Москвитин И.А., Смирнов А.А. Способ передачи информации в системах с кодовым разделением каналов и устройство для его осуществления // Патент на изобретение RU2234191 C2, опубл. 10.08.2004. — URL: http://elibrary.ru/item.asp?id=37941753 (дата обращения 28.06.2020).
18. Жук А.П., Студеникин А.В., Жук Е.П. Алгоритм и устройство формирования ансамблей псевдослучайных ортогональных последовательностей для систем передачи информации с кодовым разделением каналов // Системы управления, связи и безопасности 2020 № 3. С. 1–21. DOI: 10.24411/2410–9916–2020–10301.
19. Жук А.П., Белан Н.В., Карасев И.В., Луганская Л.А. Оценка количества ансамблей новых многофазных ортогональных сигналов // Инфокоммуникационные технологии. 2017. Том 15. № 2. С. 117–123.

20. Жук А.П., Сазонов В.В. Влияние коэффициентов второй диагонали эрмитовой матрицы на корреляционные и спектральные свойства определяемых ею ортогональных в усиленном смысле сигналов. // Физика волновых процессов и радиотехнические системы. 2007. Т. 10. № 6. С. 52–54.
21. Жук А.П., Петренко В.И., Кузьминов Ю.В., Жук Е.П., Луганская Л.А. Совершенствование способов обмена информацией в высокоскоростных беспроводных информационных сетях с использованием новых типов ансамблей дискретных последовательностей // Современные проблемы науки и образования. 2013. № 5. С. 144–153.
22. Жук А.П., Жук Е.П., Трошков А.М. Способ передачи информации с псевдослучайной перестройкой формы сигналов для систем связи с кодовым разделением каналов // Информационная безопасность. 2012: материалы XII Международной научно-практической конференции. Ч. 1.— Таганрог: ТТИ ЮФУ. 2012.— С. 346.
23. Свидетельство об гос. регистрации программы для ЭВМ № 2020665609. Программа генерации стохастических ортогональных сигналов «Stohastic orthogonal signal generator (SOSG)», 2020 г. / Сухоруков С.Ю., Жук А.П., Тран Е.С., Шуляк Я.В., Жук Е.П., Студеникин А.В.; № 2020665609; заявл. 20.11.2020; опубл. 27.11.2020.
24. Студеникин А.В., Жук А.П., Жук Е.П. Математическое моделирование ансамблей дискретных ортогональных последовательностей // Инновационные векторы цифровизации экономики и образования в регионах России, март 10–11, Ставрополь, Ставропольский государственный аграрный университет. Ставрополь: Изд-во Агрус Ставропольского гос. аграрного университета. 2021.— С. 799.
25. Жук А.П., Черняк З.В., Сазонов В.В. О целесообразности использования ансамблей ортогональных сигналов с изменяющейся размерностью в системе CDMA // Известия ЮФУ. Технические науки. 2008. № 8 (85). С. 190–195.



Журнал «Современная наука: актуальные проблемы теории и практики»


Северо-Кавказский Федеральный университет