

УДК 621.391; 004.021

В.В. Подольцев, И.М. Ажмухамедов

ОЦЕНКА ЭФФЕКТИВНОСТИ СИНХРОНИЗАЦИИ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ МАЖОРИТАРНОГО АЛГОРИТМА ПРИ ВОЗРАСТАНИИ ДЕСТРУКТИВНЫХ ОШИБОК

Подольцев Виктор Владимирович, окончил Военно-космическую академию им. А.Ф. Можайского, аспирант Астраханского государственного технического университета. Область научных интересов: обработка информации, синхронизация, помехоустойчивость. [e-mail: pvv_001@mail.ru].

Ажмухамедов Искандар Маратович, доктор технических наук, профессор, окончил Казанский государственный университет им. В.И. Ульянова-Ленина. Заведующий кафедрой «Информационная безопасность» Астраханского государственного университета. Область научных интересов: обработка информации, синхронизация, помехоустойчивость. [e-mail: aim_agtu@mail.ru].

Аннотация

Несмотря на достаточно солидный срок, проблема синхронизации псевдослучайных последовательностей (ПСП) до сих пор остается актуальной. Во-первых, это связано с широкой коммерциализацией технологий распределенного спектра, начатой еще в конце 70-х годов XX века [1] с внедрения систем мобильной телефонной связи, и продолжающимся их развитием с целью повышения эффективности [2]. Во-вторых, актуальность проблемы можно связать с появлением передовых методов множественного доступа, значительно повышающих производительность media access control (MAC) протоколов за счет применения ПСП. Таким образом, использование ПСП-ориентированных MAC-протоколов в системах обработки информации является актуальным и наиболее перспективным направлением развития информационных технологий в условиях широкой информатизации страны при переходе к цифровой экономике.

Целью работы является оценка эффективности синхронизации ПСП на основе мажоритарного алгоритма при возрастании деструктивных ошибок и обоснование задач дальнейшего исследования. В работе использованы следующие методы: метод Уорда (по «зачетному отрезку»), метод синхронизации на основе мажоритарной обработки сегментов ПСП. Показано, что мажоритарный метод дает выигрыш в помехоустойчивости за счет исправления ошибок в зачетном отрезке, по сравнению с методом Уорда, и может быть легко реализован на подуровне доступа к среде передачи MAC. Также рассмотрен метод синхронизации на основе мажоритарной обработки сегментов ПСП. Обоснована актуальность применения подобных методов на подуровне MAC-протоколов. Также в работе обоснованы цели и актуальные задачи дальнейшего исследования: оценка временных характеристик метода синхронизации на основе мажоритарных проверок; оценка вероятностных характеристик метода при условии, что система обработки информации синхронизируется по короткому сегменту ПСП; модификация метода на основе полученных результатов с целью повышения его эффективности при возрастании вероятности деструктивных ошибок в системах обработки информации и управления с ПСП-ориентированными MAC-протоколами множественного доступа.

Ключевые слова: обработка информации, среднее время поиска, вероятность деструктивной ошибки, методы синхронизации псевдослучайных последовательностей, метод мажоритарной обработки информации, метод Уорда.

doi: 10.35752/1991-2927-2020-1-5-121-126

EVALUATION OF THE EFFICIENCY OF SYNCHRONIZING PSEUDORANDOM SEQUENCES ON THE BASIS OF MAJORITY ALGORITHM AT THE DEVELOPMENT OF DESTRUCTIVE ERRORS

Viktor Vladimirovich Podoltsev, graduated from the A.F. Mozhaysky's Military Space Academy in 2009; Postgraduate Student of the Astrakhan State Technical University; research interests are in the field of information processing, synchronization, noise immunity. e-mail: pvv_001@mail.ru.

Iskandar Maratovich Azhmukhamedov, Doctor of Sciences in Engineering, Professor; graduated from Kazan State University named after V.I. Ulyanov-Lenin; Head of the Information Security Department of the Astrakhan State University; research interests are in the field of information processing, synchronization, noise immunity. e-mail: aim_agtu@mail.ru.

Abstract

Despite a substantial period of time, the problem of pseudo-random sequences (PRS) synchronization still remains topical. First, this is due to the wide technologies commercialization of distributed spectrum started in the late 70-s of XX century [1] by introduction of mobile telephone systems, and due to continued development aimed at increased efficiency [2]. Secondly, the urgency of the problem can be connected to the implementation of advanced methods of multiple accesses, greatly increasing the performance of media access control (MAC) protocols using PRS. Thus, the use of PRS-oriented MAC protocols in the information processing systems is topical and the most promising tendency of information technology development under informatization conditions in country during the transition to a digital economy. The paper aims at evaluating the effectiveness of PRS synchronization on the basis of majority algorithm with increasing destructive errors and at justification of objectives for further research. The paper deals with the following methods: Ward's method (for 'valid interval'), the synchronization method based on a majority of the processing segments of the PRS. It is shown that the majority method is beneficial for noise immunity by correcting errors in the valid interval, in comparison with Ward's method and can be easily implemented at sub-level access to the transmission medium MAC. Also the paper considers the synchronization method based on a majority of the processing segments of the PRS. It justifies urgency of such techniques at sub-level of MAC protocols. The article also describes goals and topical objectives of further study viz. evaluation of time characteristics of the synchronization method based on the majority of checks; evaluation of probabilistic characteristics method, providing that the information processing system is synchronized by a short segment of PRS; method modification based on obtained results for the purpose of improving its efficiency by increased probability of destructive errors in information processing and control systems using PRS-oriented MAC protocols of multiple access.

Key words: information processing, average search time, probability of a destructive error, methods of pseudo-random sequence synchronization, method of majority information processing, Ward's method.

ВВЕДЕНИЕ

Как правило, при рассмотрении производительности приемника или демодулятора предполагается наличие некоторого уровня синхронизации сигнала, хотя явно это высказывается не всегда. Например, при когерентной фазовой демодуляции (схема phase-shift keying (PSK)) предполагается, что приемник может генерировать опорные сигналы, фаза которых идентична (возможно, с точностью до постоянного смещения) фазе элементов сигнального алфавита передатчика. Затем в процессе принятия решения относительно значения принятого символа (по принципу максимального правдоподобия) опорные сигналы сравниваются с поступающими.

При генерации подобных опорных сигналов приемник должен быть синхронизирован с принимаемой несущей частотой. Это означает, что фаза поступающей несущей частоты и ее копии в приемнике должны согласовываться. Другими словами, если в поступающей несущей частоте не закодирована информация, поступающая несущая и ее копия в приемнике, будут проходить через нуль одновременно. Этот процесс называется фазовой автоподстройкой частоты (это условие, которое следует удовлетворить максимально близко, если в приемнике мы хотим точно демодулировать когерентно модулированные сигналы). В результате фазовой автоподстройки частоты местный гетеродин приемника синхронизируется по частоте и фазе с принятым сигналом.

В соответствии с семиуровневой иерархической моделью телеметрических служб (open systems interconnection (OSI)) управление доступом к среде (media access control (MAC)) осуществляется на втором канальном уровне – подуровне управления доступом к среде (MAC).

MAC является одним из расширений модели OSI. Институт инженеров по электротехнике и радиоэлектронике разделяет канальный уровень на два подуровня: подуровень управления доступом к среде (MAC) и подуровень управления логической связью (logical link control (LLC)), из которых нижним является MAC. Таким образом, MAC выступает в качестве интерфейса между подуровнем LLC и физическим (первым) уровнем.

MAC обеспечивает адресацию и механизмы управления доступом к каналам, что позволяет нескольким терминалам или точкам доступа общаться между собой в многоточечной сети (например, в локальной или городской вычислительной сети), и эмулирует полнодуплексный логический канал связи в многоточечной сети.

Этот уровень используется для того, чтобы передать не просто биты, а осмысленные последовательности из этих бит. Используется для передачи данных в одной канальной среде. На этом уровне работают MAC-адреса, которые еще называют физическими адресами. Термин «физические адреса» ввели не просто так. Каждая сетевая карта или антенна имеет вшитый адрес, который ей присваивает производитель.

Большинство методов синхронной обработки информации в ПСП-ориентированных MAC-протоколах множественного доступа, как правило, разрабатываются для реализации на физическом уровне и фактически сложны или нереализуемы на подуровне доступа к среде передачи MAC, где протоколы множественного доступа оперируют с уже принятыми и декодированными битовыми последовательностями. Однако с учетом специфики функционирования ПСП-ориентированных протоколов множественного доступа, автором было найдено малое число работ [3].

Существует синхронизация ПСП по методу Уорда и другие модификации метода Уорда, которые можно реализовать на подуровне доступа к среде передачи MAC. Так в работе [4] предложен мажоритарный метод синхронизации ПСП, использование которого повышает вероятность синхронизации ПСП. Недостатком метода является значительное повышение вычислительной сложности с увеличением длины линейного рекуррентного регистра. Данный недостаток был решен в работе [5], в которой рассматривается метод мажоритарного декодирования m -последовательности, требующий меньших аппаратных затрат. В работе [6] на базе данного метода декодирования был предложен метод синхронизации ПСП. Преимуществами метода являются:

- высокая помехоустойчивость;
- низкая аппаратная сложность;
- возможность применения его в системах обработки информации с ПСП-ориентированными протоколами множественного доступа.

Поэтому данный метод может быть легко реализован в подобных системах обработки информации. Рассмотрим данный метод подробнее и проведем системный анализ его эффективности при возрастании деструктивных ошибок.

МЕТОД МАЖОРИТАРНОЙ ОБРАБОТКИ ИНФОРМАЦИИ ПРИ СИНХРОНИЗАЦИИ ПСП

Одной из особенностей m -последовательностей является их большая избыточность. Это свойство позволяет относительно каждого символа m последовательности составить систему проверочных уравнений (проверок) следующего вида [5]:

$$a_j^{(l)} = \sum_{i=1}^N C_{ij}^{(l)} \cdot a_i, \tag{1}$$

где $N = 2^k - 1$; $j = 1, 2, \dots, k$ – номер декодируемого символа; l – номер проверочного уравнения; a_j, a_i – символы кодового слова; $C_{ij}^{(l)}$ – коэффициенты поля Галуа $GF(2)$; k – длина линейного рекуррентного регистра (ЛРР).

По большинству проверок вида:

$$T_{cp} = \frac{(2 - P_D)(1 + KP_{ЛС})}{P_D} (M_c \lambda T_c), \tag{2}$$

где λT_c – интервал поиска; P_D – вероятность правильного детектирования; M_c – количество элементарных сигналов; $P_{ЛС}$ – вероятность ложной синхронизации; $K \gg 1$, можно с высокой достоверностью принять решение о значении принимаемого символа. На этом свойстве основаны известные методы мажоритарного приема (декодирования) m последовательностей [5].

Проверочную матрицу m -последовательности $H = [P^T I]$ за счет ее свойства цикличности можно легко привести к виду:

$$H' = [IP^T], \tag{3}$$

где I – единичная подматрица.

Пусть первые « k » символов принимаемой ПСП определяют начальную фазу φ_0 . Тогда при поступлении очередного символа получим следующие « k » символов, которые определяют фазу φ_1 и т. д. Если H' :

$$T_{cp} = \frac{1 - q^k}{Pq^n U}, \tag{4}$$

где k – число успехов (длина «зачетного отрезка»); U – скорость передачи; P – вероятность деструктивной ошибки; $q = 1 - P$ – вероятность правильного приема одного чипа, записать в развернутом виде, то легко заметить, что последняя строка будет задавать соотношение, связывающее фазу φ_0 с « k » символами фазы φ_1 ; предпоследняя строка будет задавать соотношение, связывающее фазу φ_0 с « k » символами φ_2 и т. д. Строки P^T просто генерируются регистром со встроенными сумматорами, соединенными в соответствии порождающим полиномом $h(x)$ и работающим в обратном направлении. Тогда модифицированный мажоритарный алгоритм можно представить следующим образом:

$$\varphi_0 = \varphi_l [\alpha^{-l} \alpha^{-l+i} \dots \alpha^{-l+k-1}], \tag{5}$$

где α^{-l+i} – вектор столбца матрицы.

На рисунке 1 представлена схема устройства синхронизации ПСП на основе модифицированного мажоритарного алгоритма.

Устройство синхронизации ПСП на основе мажоритарного алгоритма состоит из следующих элементов:

- генератора элементов поля α ;
- приемного регистра φ_i ;
- ключевых схем на элементах «И»;
- сумматора по модулю два на « K » входов;
- коммутатора;
- « K » счетчиков с пороговыми элементами;
- датчика ПСП;
- блока управления;
- схемы подгона;
- коррелятора.

За один такт работы приемного регистра φ_i генератор поля α должен проработать « k » тактов, при этом последовательно будут формироваться символы

a_1, a_2, \dots, a_k . Действительно, если для первых « k » символов состояние генератора поля принять a^0 , то, сдвигая его вправо, получим последовательно состояния $\alpha^1, \alpha^2, \dots, \alpha^{k-1}$, которые, включая α^0 , дадут на выходе сумматора соответственно: a_1, a_2, \dots, a_k . При приеме очередного символа состояние генератора поля будет соответствовать α^{-1} , что даст на выходе сумматора символ a_1 и при последовательных сдвигах генератора вправо получим a_2, \dots, a_k . В пороговых схемах будут накапливаться значения a_i и при превышении заданного порога параллельно выдается решение о значении фазы φ_0 (рис. 1).

Синхронизация ПСП обеспечивается подгоном на величину задержки, равной величине порога, и последующей проверкой корреляционным методом правильности синхронизации. Действительно, современные программируемые логические интегральные схемы позволяют создавать генераторы ПСП, работающие со скоростью порядка 20 Гчип/с, в то время как чиповая скорость в системах связи широкополосного доступа составляет порядка 30 Мчип/с. Соответственно, при обработке сегмента ПСП менее 1000 чипов время на подгон составит не более длительности одного канального чипа.

Для систем с MC-CDMA в работах [7, 8] предложена модификация известного мажоритарного метода, схема устройства которого представлена на рисунке 2.

Для простоты реализации на приеме решающее устройство (РУ) так же, как и декодирование ПСП, работает по мажоритарному алгоритму, принимая решение по большинству принятых элементов ПСП.

Помехоустойчивость метода оценена с использованием Гауссовской аппроксимации с учетом независимости проверок [6]:

$$P_{out}(k) = 1 - \left[1 - F \left(\frac{\sum_{i=1}^k W_i J_i N (2P_i - 1)}{2 \sqrt{\sum_{i=1}^k W_i^2 P_i (1 - P_i) J_i N (2^k - 1)}} \right) \right]^k, \quad (6)$$

где $W_i = \lg((1 - P_i)/P_i)$ – вес проверки размерности i ; N – длина сегмента ПСП; $J_i = C_{k-1}^{i-1}$ – число проверок размерности i в одном периоде ПСП; $P_i = (1 - (1 - 2P_{cp})^i)/2$ – вероятность ошибки в проверке размерности i ; k – длина линейного рекуррентного регистра; $F(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-t^2/2} dt$ – интеграл вероятности.

Для схемы, представленной на рисунке 2, среднюю вероятность деструктивной ошибки P_{cp} можно рассчитать по следующей формуле:

$$P_{cp} = \sum_{k=\frac{Nc+1}{2}}^{Nc} C_{Nc}^k P^k (1-P)^{Nc-k}, \quad (7)$$

где P – вероятность ошибки на одной поднесущей; Nc – количество поднесущих.

Для вероятности неприема синхронизирующей информации по методу Уорда будет справедлива оценка [6]:

$$P_u = [1 - (1 - P)^n]^Z, \quad (8)$$

где $Z = N/n$ – количество непересекающихся «зачетных отрезков»; P – вероятность ошибки в канале связи.

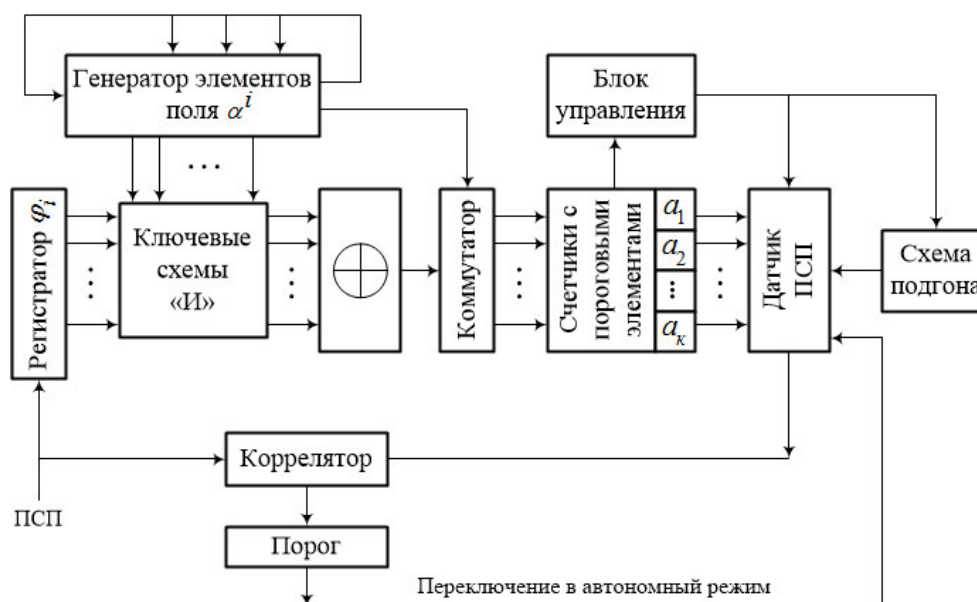


Рис. 1. Схема устройства синхронизации ПСП на основе мажоритарного алгоритма [6]

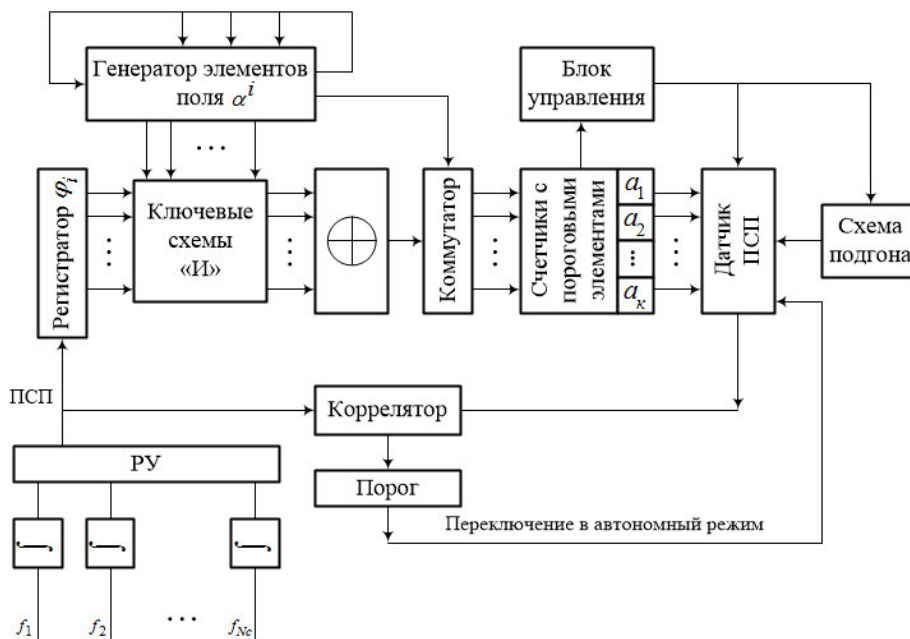


Рис. 2. Схема устройства синхронизации ПСП на основе модифицированного мажоритарного алгоритма для MC-CDMA

Исследуем эффективность разработанного модифицированного мажоритарного метода по сравнению с методом Уорда. На рисунке 3 представлены зависимости вероятности ошибки приема одного бита ПСП для метода Уорда (метод по «зачетному отрезку» (ЗОТ)) и мажоритарного метода, рассчитанного по формулам (6) и (8) при длине ЛРР – 10, длине сегмента ПСП – 25.

Для метода Уорда вероятность битовой ошибки принималась равной вероятности деструктивной ошибки. Анализ зависимостей показывает, что модифицированный мажоритарный метод, показанный на рисунке 2, дает значительный выигрыш, в сравнении

с методом Уорда, при возрастании вероятности деструктивной ошибки в канале связи. Так, как видно из графиков, выигрыш мажоритарного метода при вероятности деструктивной ошибки 0,1 составляет шесть порядков.

На рисунке 4 представлена зависимость вероятности неприема символа ПСП мажоритарного метода от длины обрабатываемого сегмента ПСП.

Анализ зависимости показывает, что увеличение длины обрабатываемого сегмента может значительно повысить вероятность правильного приема ПСП. Как видно из графика, пятикратное увеличение длины сег-

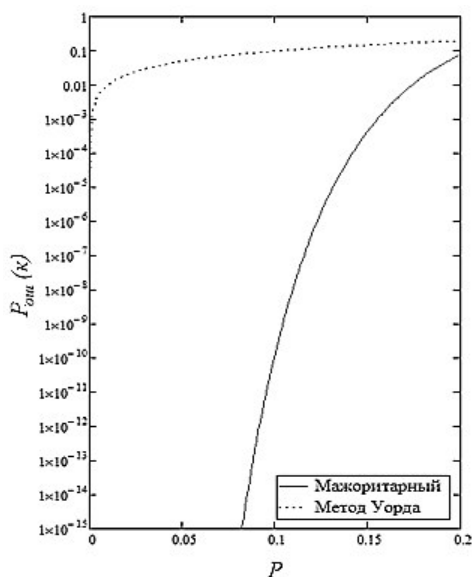


Рис. 3. Зависимость вероятности ошибки приема одного бита ПСП P_{oui} от вероятности деструктивной ошибки P

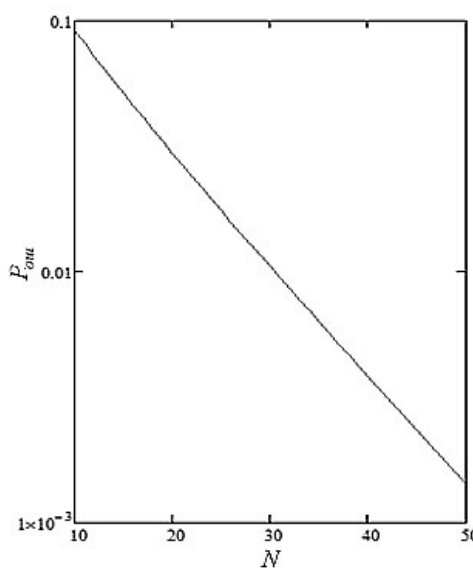


Рис. 4. Зависимость вероятности неприема символа ПСП мажоритарного метода P_{oui} от длины обрабатываемого сегмента ПСП N

мента ПСП снижает вероятность битовой ошибки на два порядка с 10^{-1} до 10^{-3} .

Аппаратная сложность разработанного мажоритарного метода, как показано в работе [6], изменяется по логарифмическому закону и требует меньшего количества памяти для его реализации в сравнении с оптимальными методами и методом Уорда.

Впервые, в отличие от известных работ [4], проведено исследование не только вероятностных, но и временных характеристик по разработанным формулам (3) и (4) модифицированного мажоритарного алгоритма, изображенного на рисунке 2, что позволяет оценить выигрыш по времени синхронизации при использовании разработанного на уровне изобретения модифицированного мажоритарного алгоритма, в сравнении с другими методами, которые могут быть реализованы на подуровне MAC.

ЗАКЛЮЧЕНИЕ

Таким образом, теоретическая и практическая новизна работы заключается в том, что впервые разработана на уровне изобретения структурная схема модифицированного мажоритарного алгоритма для MC-CDMA, которая в отличие от известных методов позволяет принимать решение по большинству принятых элементов ПСП. Также разработана методика расчета длины синхропоследовательности при модифицированной мажоритарной обработке сегмента ПСП с целью снижения времени синхронизации в условиях деструктивных ошибок.

СПИСОК ЛИТЕРАТУРЫ

1. Ipatov V. *Spread Spectrum and CDMA Principles and Applications*. University of Turku and Saint Petersburg Electrotechnical University «LETI», John Wiley & Son, 2005. 400 p.
2. Попов В.И. Основы сотовой связи стандарта GSM. М.: Экотрендз, 2005. 296 с.
3. Лощкарев А.В. Применение M-последовательностей для обеспечения помехоустойчивости и синхронизации в беспроводных сетях // Сб. тр. Рос. науч.-техн. конф. «Современные проблемы телекоммуникаций». Новосибирск, 2014. С. 61–62.
4. Kilgus C. Pseudonoise code acquisition majority logic decoding // *IEEE Trans. on Communication*, COM-21, 1973. № 6. pp. 772–774.
5. К вопросу о мажоритарном декодировании M-последовательностей / И.А. Новиков, В.Н. Номоконов, А.А. Шебанов [и др.] // *Вопросы радиоэлектроники*. Сер. ОТ. 1976. Вып. 5. С. 50–55.
6. Хисамов Д.Ф. Моделирование процесса синхронизации датчиков псевдослучайных последовательностей в подавляемых системах радиосвязи : дисс. ... канд. техн. наук. Воронеж. институт МВД России, Воронеж, 2005. 154 с.
7. Исследование алгоритма синхронизации ПСП для систем связи с многочастотными сигналами с помощью компьютерного моделирования / В.И. Лойко, Ф.Г. Хисамов, М.В. Милованов, А.Д. Золотуев // *Научный журнал КубГАУ*. Краснодар : КубГАУ, 2015. № 111 (07). С. 47–52.
8. Пат. 2604345 РФ, МПК H04W 56/00. Устройство синхронизации псевдослучайной последовательности для систем связи с многочастотными сигналами / Хисамов Ф.Г., Подольцев В.В., Хисамов Д.Ф., Собачкин Д.М., Золотуев А.Д., Милованов М.В. – № 2015137562/08 ; заявл. 02.09.2015 ; опубл. 10.12.2016, Бюл. № 34. 1 с.

REFERENCES

1. Ipatov V. *Spread Spectrum and CDMA Principles and Applications*. University of Turku and Saint Petersburg Electrotechnical University 'LETI', John Wiley & Son Publ., 2005. 400 p.
2. Popov V.I. *Osnovy sotovoi svyazi standarta GSM* [The basics of cellular standard GSM]. Moscow, Ekotrendz Publ., 2005. 296 p.
3. Loshkarev A.V. *Primenenie M-posledovatelnoستي dlia obespecheniia pomekhoustoichivosti i sinkhronizatsii v besprovodnykh setiakh* [The use of M-sequences to provide noise immunity and synchronization in wireless networks]. *Sbornik trudov Ros. nauch.-tekhn. konf. 'Sovremennye problemi telekommunikatsii* [Proc. of Russian Sci.-Tech. Conf. on Present-day Telecommunication Issues], Novosibirsk, 2014, pp. 61–62.
4. Kilgus C. Pseudonoise Code Acquisition Majority Logic Decoding. *IEEE Trans. on Communications*, 1973, vol. COM-21, no. 6, pp. 772–774.
5. Novikov I.A., Nomokonov V.N., Shebanov A.A. *Kvoprosu o mazhoritarnom dekodirovanii M-posledovatelnoستي* [On the Question of Majority Decoding of M-sequences]. *Voprosi radioelektroniki. Ser. OT* [Radio Electronic Issues. Gen. Tech. Ser.], 1976, iss. 5, pp. 50–55.
6. Khisamov D.F. *Modelirovanie protsessa sinkhronizatsii datchikov psevdosluchainykh posledovatelnoستي v podavlyaemykh sistemakh radiosvyazi. Diss, kand. Tekhn. nauk* [Modeling the Process of Synchronization of Pseudo-Random Sequence Sensors in Suppressed Radio Communication Systems]. Voronezh, Institute of Min. of Int. of Russia Publ., 2005. 154 p.
7. Loiko V.I., Khisamov F.G., Milovanov M.V., Zolotuev A.D. *Issledovanie algoritma sinkhronizatsii PSP dlia sistem svyazi s mnogochastotnymi signalami s pomoshchiu kompiuternogo modelirovaniia* [Study of the PSP Synchronization Algorithm for Communication Systems with Multi-Frequency Signals Using Computer Simulation]. *Nauchnyi zhurnal KubGAU* [Scientific Review of KubSAU], 2015, no. 111(07), pp. 47–52.
8. Russian Federation Patent 2604345 RF, MPK H04W 56/00. *Ustroistvo sinkhronizatsii psevdosluchainoi posledovatelnoستي dlia sistem svyazi s mnogochastotnymi signalami* [Pseudo-Random Sequence Synchronization Device for Communication Systems with Multi-Frequency Signals]. Inventors: Hisamov F.G., Podoltsev V.V., Hisamov D.F., Sobachkin D.M., Zolotuev A.D., Milovanov M.V. Application: 2015137562/08. Date of filing: September 02, 2015. Date of publication: December 10, 2016, Bull. 34, 1 p.