бок в СОК, показан способ восстановления информации без коррекции ошибок. Разработано программное обеспечение для моделирования группового разделения секрета на примере разделения цветного изображения с локализацией ошибок. На программной модели показано, что для восстановления секрета групповым методом допустимо потерять больше частей информации, чем при использовании линейного метода. Показана возможность применения разработанной модели для криптографической и некриптографической защиты информации. Работа выполнена при поддержке РФФИ, проект № 13-07-00478-а.

Литература

1. Червяков Н.И., Сахнюк П.А., Шапошников А.В. и др. Нейрокомпьютеры в остаточных классах. Кн. 11. М.: Радиотехника, 2003. – 272 с.
2. Червяков Н.И., Евдокимов А.А. Галушкин А.И. и др. Применение искусственных нейронных сетей и систем остаточных классов в криптографии. М.: Физматлит, 2012. – 280 с.
3. Червяков Н.И., Сахнюк П.А., Шапошников А.В. и др. Модулярные параллельные вычислительные структуры нейропроцессорных систем. М.: Физматлит, 2003. – 288 с.
4. Soderstrand M.A., Jenkins W.K., Jullien G.A., Taylor F.J. Residue Number System Arithmetic: Modern Applications in Digital Signal Processing. IEEE Press, New York, 1986. – P. 15-19.
5. Патент RU № 2380751 от 30.05.2008. Нейронная сеть с пороговой (k,t) структурой для преобразования остаточного кода в двоичный позиционный код // Червяков Н.И., Головко А.Н., Лавриненко А.В. и др.
6. Акушский И.Я., Юдицкий Д.М. Машинная арифметика в остаточных классах. М.: Сов. радио, 1968. – 440 с.
7. Нестеренко А. Введение в современную криптографию. Теоретико-числовые алгоритмы. Курс лекций для вузов. img0.liveinternet.ru, 2011. – 190 с.

METHOD DEVELOPMENT NOISEPROOF SECRET SHARING BASED ON THE APPLICATION OF TWO-STAGE SYSTEM, THE RESIDUAL CLASSES

Kocherov Y.N., Chervyakov N.I.

The article presents a group method of secret sharing, based on a residue number system. When using this method increases the ability to scan for code that is increasing the number of detected errors.

Keywords: *residue number system, generalized Polyadic number system, secret sharing.*

Кочеров Юрий Николаевич, аспирант Кафедры информационных систем, электропривода и автоматики Невинномысского технологического института – Филиала Северо-Кавказского федерального университета (СКФУ). Тел. 8-865-543-55-08; 8-918-866-91-93. E-mail: kocherov_yra@mail.ru

Червяков Николай Иванович, д.т.н., профессор, Заслуженный деятель науки и техники РФ, профессор Кафедры высшей алгебры и геометрии СКФУ. Тел.: (8-865) 275-35-64. E-mail: k-fmf-primath@stavsu.ru

УДК 621.391

МЕТОД ФОРМИРОВАНИЯ МЯГКИХ РЕШЕНИЙ В СИСТЕМЕ ШИРОКОПОЛОСНОГО КАНАЛА СВЯЗИ С НЕЗВЕСТНЫМИ ПАРАМЕТРАМИ ОСТАТОЧНЫХ КЛАССОВ

Баскакова Е.С., Гладких А.А.

Решается задача формирования индексов мягких решений (ИМР) символов применительно к технологии обработки сигналов в системе с ортогональным частотным мультиплексированием (OFDM), использующей каналы с неизвестными параметрами. Задачи подобного типа являются актуальными при обмене данными систем реального времени в ходе оперативного взаимодействия двух или нескольких подвижных объектов при применении в них широкополосных систем связи. Метод вычисления ИМР основан на критерии минимума евклидовой метрики.

Ключевые слова: мягкое декодирование, итеративный процесс, стирание, технология OFDM, логарифм отношения правдоподобия.

Введение

В последнее время широкое распространение получили системы цифровой связи, использующие многочастотную модуляцию. Это обусловлено такими их достоинствами, как возможность подавления межсимвольной интерференции сравнительно простыми в вычислительном отношении средствами, возможность использования в передатчике и приемнике эффективных алгоритмов быстрого преобразования Фурье, возможность гибко адаптировать распределение мощности и информационной нагрузки по частотам.

Системы с многочастотной модуляцией делятся на два класса. Термин «ортогональное частотное мультиплексирование» (Orthogonal Frequency Division Multiplexing – OFDM) обычно применяется для систем радиосвязи, в которых мощность и число бит в символе являются одинаковыми для всех поднесущих, а цифровое формирование сигнала производится на уровне комплексной огибающей с последующим квадратурным переносом на несущую частоту.

Вторая разновидность таких систем, обозначаемая термином «дискретная многочастотная модуляция» (Discrete MultiTone – DMT), подразумевает использование проводного канала связи и гибкое управление распределением мощности и информационной нагрузки по частотам в зависимости от свойств конкретного канала связи [1-2].

Для достижения требуемого уровня достоверности в подобных системах необходимо применение средств помехоустойчивого кодирования, и по объективным причинам в наибольшей степени это оправданно для технологии с OFDM. Максимально правдоподобное декодирование QAM-сигналов эквивалентно нахождению ближайшей точки созвездия к точке принятого сигнала, а степень отклонения в евклидовой метрике может служить мерой мягкого решения. Важно отметить, что в системах DMT с относительно стабильными параметрами и большими объемами передаваемых данных в качестве мягких решений с успехом используется классический метод логарифма отношения правдоподобия. В условиях применения OFDM такой метод с высокой вероятностью приводит к недостоверным данным из-за отсутствия сведений о параметрах канала связи. Целью работы является разработка метода формирования ИМР в условиях применения QAM в каналах с априорной неопределенностью о значениях их параметров.

Постановка задачи

В большинстве аналитических оценок эффективности процедуры мягкого декодирования помехоустойчивых кодов в качестве ИМР-символов принимается логарифм отношения правдоподобия (Log Likelihood Ratio – LLR) [1-4]. Значение этого параметра для двоичных систем модуляции определяется как

$$L(u_i \mid \bar{z}) = \ln\left[\frac{P(u_i = +1 \mid \bar{z})}{P(u_i = -1 \mid \bar{z})}\right], \quad (1)$$

где $u_i = \pm 1$ – возможные значения бита, а $\bar{z}$ – принятая приемником последовательность бит. Для одного принятого символа $z_i = \pm 1$, а значение LLR для канала с независимым потоком ошибок в условиях применения двоичной фазовой модуляции определятся выражением

$$L(u_i \mid z_i) = \ln\left[\frac{P(u_i \mid z_i = +1)}{P(u_i \mid z_i = -1)}\right] = \frac{2\sqrt{E_b} z_i}{\sigma^2}, \quad (2)$$

где E_b – энергия сигнала, приходящаяся на бит, σ^2 – дисперсия шума.

В случае применения каналов с общими замираниями и коэффициентом затухания α выражение для LLR принимает вид

$$L(u_i \mid z_i) = \frac{2\sqrt{E_b} z_i}{\sigma_i^2} \times \alpha_i. \quad (3)$$

При реализации мягкого декодирования помехоустойчивого кода необходимо вычислить LLR для каждого бита. Но в [7] было показано, что выражения (2) и (3) невозможно использовать для каналов с нестационарными параметрами. Действительно, положим в (3) $\alpha = 1$ (гауссовский канал с аддитивным шумом), $\sigma_i^2 = 1$, $E_b = 1$ и $z_i = 0{,}5$, тогда заданная конфигурация параметров будет соответствовать уровню соотношения «сигнал-шум» в 3дБ, в то время как при неизменных значениях $E_b, z_i = z_j$, но $\sigma_j^2 = 0{,}1$ соотношение сигнал-шум составит 13 дБ и значения LLR окажутся разными при одном и том же уровне принятого сигнала. В первом случае значение LLR оказывается равным $L(u_i \mid z_i) = 1$, а во втором случае $L(u_j \mid z_j) = 10$. Естественно, разброс параметров ИМР отрицательно сказывается на реализации процессора приемника, отвечающего за процедуру мягкого декодирования помехоустойчивого кода. Кроме того, статистика LLR не может быть использована в системе обмена данными для оценки параметров канала связи,

например, для адаптивного управления параметрами на отдельных поднесущих в OFDM.

В [1] LLR оценивается применительно к технологии DMT и КАМ. Для канала связи с аддитивным белым гауссовым шумом при равных априорных вероятностях нуля и единицы LLR бита для одной несущей частоты равен

$$LLR(u_i \mid \dot{z}_i) \approx \ln \frac{\max \exp(-\left|\dot{z}_i - C_{m=1}\right|^2 / 2\sigma^2)}{\max \exp(-\left|\dot{z}_i - C_{m=0}\right|^2 / 2\sigma^2)}, \quad (4)$$

где $C_{m=1}$ и $C_{m=0}$ – подмножества точек сигнального созвездия КАМ, для которых u_i в совокупности имеет показатели 0 и 1 соответственно, ближайшие к принятому из канала значению сигнала $\dot{z}_i$, m – номер OFDM символа.

В (4) в качестве одного из параметров также входит значение дисперсии шума σ^2. Следовательно, для определения LLR требуется знание параметров канала связи или их предварительное измерение в расчете на сохранение стационарности показателей мешающих факторов в ходе сеанса обмена данными.

В условиях применения OFDM реализация последнего требования для отдельных поднесущих из заявленного в системе множества является невыполнимой. Поэтому возникает целесообразность разработки такого метода вычисления мягких решений в системе OFDM, который позволял бы определять этот параметр без знания характеристик канала связи, как это было предложено для двоичного канала в [7]. В этом случае мягкие решения получили наименование ИМР.

Роль точной оценки мощности шума в процедуре мягкого декодирования избыточных кодов

Влияние неточности определения мощности шума на характеристики помехоустойчивости производилось в [8]. Среди перспективных алгоритмом мягкой обработки помехоустойчивых кодов выделяют алгоритм Витерби с мягким выходом – SOVA [1-3], Log-MAP алгоритм [3-5, 8], Max-Log-MAP алгоритм [3-4, 8] и алгоритм, основанный на упорядоченных оценках надежности декодированных символов SO-OSD[3-5]. Исследованиями, проведенными в [8], показано, что алгоритмы SOVA и Max-Log-MAP не зависят от правильности оценки мощности шума из-за свойства линейности этих алгоритмов.

В то же время точность оценки надежности канала оказывает существенное влияние на эффективность турбодекодера с алгоритмом декодирования вида Log-MAP, работающего в составе турбодекодера. Отсутствие данных об уровне мешающих факторов в канале связи в таком алгоритме не дает практически значимого энергетического выигрыша в системе связи при любом числе итераций. Эффективность турбокодеров кодов растет с увеличение длины кадра, что не всегда приемлемо для систем передачи коротких управляющих сигналов, например систем корректировки навигационных данных или команд управления. Известно, что алгоритм Max-Log-MAP является модификацией процедуры Log-MAP, обладает меньшей вычислительной сложностью, но теряет свойство оптимальности.

Данные, представленные в [5], показывают, что алгоритм SO-OSD удобен для обработки коротких блоковых кодов, вероятность ошибки этого алгоритма совпадает с вероятностью ошибки по Max-Log-MAP, и уменьшение масштаба ИМР способствует получению дополнительного энергетического выигрыша. Этот фактор говорит о целесообразности применения в таких системах целочисленных ИМР [2]. Именно такие системы оптимальны в системе корректировки данных управления реального времени по критерию скорости обработки и защиты от помех антропогенного характера за счет случайного времени начала сеанса связи. С увеличение длин кода в таком алгоритме неопределенность уровня шума приводит к снижению вероятности определения наиболее вероятного кодового слова за счет неточного перехода к эквивалентному коду при итеративных преобразованиях символов. Таким образом, применение алгоритма SO-OSD для своей реализации требует знания параметра отношения «сигнал-шум».

Процедура вычисления дисперсии шума и помех при приеме сигналов OFDM

Основой большинства известных алгоритмов оценки дисперсии помехи является усреднение квадрата модуля разности между комплексной амплитудой принятого сигнала и ее оценкой. Действительно, многие оптимальные алгоритмы обработки сигналов OFDM требуют предварительной оценки дисперсии шума и помехи. В частности, подобная задача возникает при оценке и компенсации влияния распространения сигнала по многолучевому канала. Для оценки названного параметра оценивается доплеровская спектральная плотность мощности канала

с использованием опорных (пилотных) поднесущих.

В частотной области комплексная амплитуда поднесущей с номером q OFDM символа m на входе приемника может быть описана как

$$a_{pr}(m,q) = H(m,q)a_{per}(m,q)\exp\left[j\varphi(m) + n(m,q)\right],$$

где $a_{per}(m,q)-$ комплексные амплитуды поднесущих передаваемого символа m; $H(m,q)$ – среднее значение частотной характеристики подканала q в ходе обработки символа m; $\varphi(m)$ – ошибка рассогласования фазы; $n(m,q)$ – отсчеты суммарной помехи от межканальной интерференции и шума в канале. Тогда дисперсия определяется как

$$\overline{\sigma}^2 = \left|a_{pr}(m,q) - \overline{a}_{pr}(m,q)\right|^2 = \left|a_{pr}(m,q) - \overline{H}(m,q) \times \overline{a}_{per}(m,q)\right|^2, \quad (5)$$

где усреднение проводится как по m, так и по q. Из (5) становится ясно, что алгоритмы требуют предварительной оценки частотной характеристики канала и значений комплексных амплитуд передаваемых поднесущих, поэтому их применение для решения рассматриваемой задачи затруднительно, а в системах с быстро изменяющимися параметрами недопустимо.

Метод вычисления ИМР в системе QPSK-QAM с неизвестными параметрами канала связи

В [7] представлена универсальная процедур формирования ИМР-символов в системах с двоичной модуляцией и намечены основные пути реализации метода для системы с QPSK. Указывается, что в зависимости от особенностей вида модуляции рабочие характеристики формирователя ИМР могут носить открытый характер или закрытый характер. В системах со сложными видами модуляции могут быть использованы обе характеристики, но в целях унификации процедуры вычисления ИМР целесообразно применять характеристику закрытого типа.

На рис. 1 представлено созвездие сигналов с кодом Грея, которое используется в системе с иерархической модуляцией. Точки созвездия QAM-16 и сигналы QPSK, обозначенные символом «×», могут быть использованы одновременно. При этом для точек QPSK используются первые два бита из нумерации QAM-16. Допускается одновременная передача указанных сигналов. Очевидно, что евклидова метрика для точек QPSK больше, поэтому эта система сигналов более помехоустойчива. Если в системе обмена данными возможно выделение более важных данных и менее важных данных, то более важные данные целесообразно передавать с использованием QPSK. Например, при использовании кластерного подхода при декодировании помехоустойчивых кодов [5] для передачи номера кластера выгодно использовать QPSK. В системе с OFDM иерархическая модуляция может быть использована в подканалах с незначительным уровнем помех.

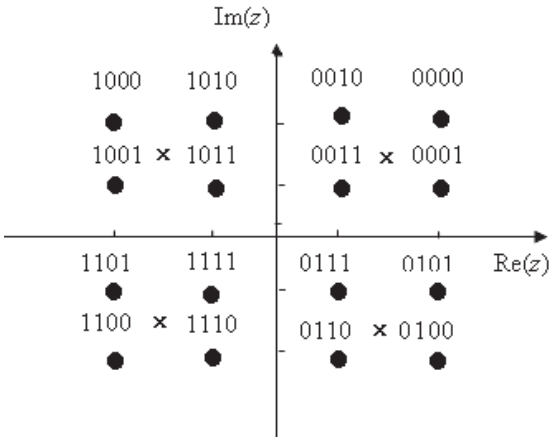

Рис. 1. Созвездие QPSK-QAM, используемое в системе с иерархической модуляцией

Алгоритм получения ИМР в системе сложных сигналов рассмотрим на примере QAM-16. На рис. 2 показана система таких сигналов, естественно, что координаты точек созвездия приемнику известны. Поэтому задача заключается в том, чтобы вычислить евклидову метрику от принятой приемником точки z (показана на рисунке в виде незатушеванной окружности) до ближайших точек созвездия. Подобная задача решается в системе сферического декодирования сигналов [8]. При этом возможно получение различных результатов. Если выполняется условие $\alpha < \beta < \gamma < \zeta$, то за метрику выбирается значение – a. В случае появления равенства в любом сочетании указанных векторов сигналу целесообразно присвоить низшую оценку из возможных.

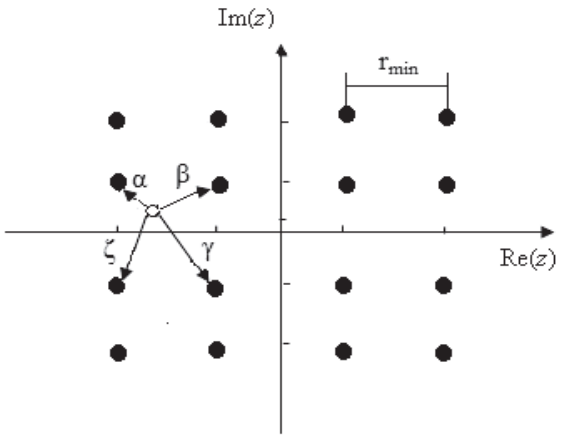

Рис. 2. Принцип определения минимума евклидовой метрики в созвездии QAM-16

Схема формирования ИМР в канале с неизвестными параметрами показана на рис. 3.

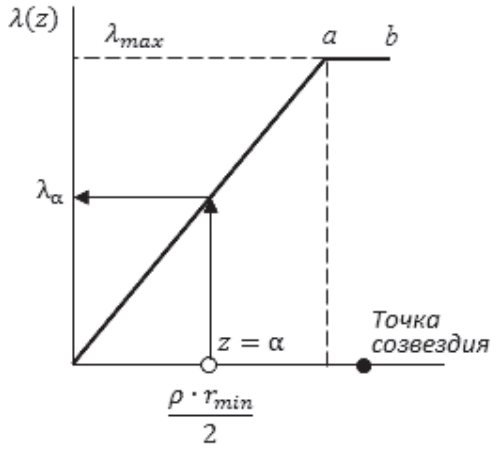

Рис. 3. Схема формирования ИМР

Расстояние *ab* определяется интервалом стирания ρ, где ρ – доля от $0 \le \rho < 1$. По сути, интервал ab определяет диаметр зоны надежной регистрации сигнала *z*. Таким образом, вычисление текущего значения ИМР λ_α осуществляется по правилу

$$|\lambda(z)| = \begin{cases} \dfrac{2\lambda_{\max}}{\rho r_{\min}} \times \alpha \quad \text{при} \quad \alpha \neq \beta \neq \gamma \neq \zeta \quad u \quad z < a; \\ \lambda_{\max} \quad \text{при} \quad a \le z \le b; \\ \lambda_{\min} = 0 \quad \text{при} \quad z > r_{\min}/2. \end{cases}$$

Применение характеристики для одной из четырех номинальных точек системы QPSK показано на рис. 4. В [7] доказано, что при учете краевого эффекта в подобной системе число достоверных ИМР со значениями $\lambda_{\max}$ может быть увеличено. В системе с QAM-16 учет краевого эффекта приводит к усложнению решающего правила, и его использование становится нецелесообразным.

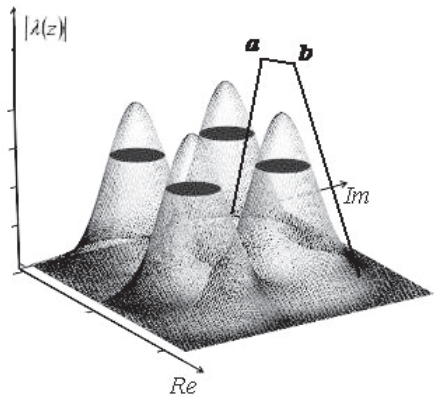

Рис. 4. Пример применения решающего правила для одной точки созвездия системы QPSK

Алгоритм вычисления ИМР сохраняется для любых значений сигналов категории QAM, в том числе и для QPSK, что в совокупности с результатами работы [7] подчеркивает универсальность правила формирования ИМР.

Выводы

1. Показано, что известные методы оценки логарифма отношения правдоподобия в качестве мягких решений в схеме декодирования помехоустойчивых кодов требуют знания параметров мешающих факторов, действующих в канале связи в формате дисперсии шума и помех. Это требование не противоречит свойствам каналов связи с относительно постоянными параметрами. В случае нестационарных каналов связи незнание дисперсии шума и помех приводит к неоднозначной оценке LLR, что снижает эффективность декодеров с итеративными преобразованиями по достижению заданного уровня энергетического выигрыша. Таким образом, вычисление LLR в каналах с неизвестными параметрами по существующим методикам затруднительно.

2. Оценка возможностей различных методов декодирования избыточных кодов показала, что методы SOVA и Max-Log-MAP наименее критичны к знанию параметра дисперсии шума, в то время как метод Log-MAP при неизвестной дисперсии совершенно не обеспечивает прироста эффективности в ходе итераций, а метод SO-OSD оказывается наиболее чувствительным к незнанию параметра шума.

3. Универсальный метод на основе стирающего канала связи с широким интервалом стирания пригоден не только для двоичных методов модуляции, но и эффективен при использовании сложных видов модуляции типа QPSK–QAM. Метод не требует знания дисперсии шума и, следовательно, эффективен для применения в каналах с неизвестными параметрами.

4. Используя статистику текущих значений ИМР, можно судить о стоянии того или иного канала системы OFDM, не прибегая к организации тестирующих пилот-сигналов, что способствует повышению спектральной эффективности используемого частотного диапазона.

Литература

1. Natalin A.B., Sergienko A.B. The Method of Theoretic Estimation of BER of ML Receiver for Binary Coded Systems with Square QAM // Proc. IEEE Int. Conf. on Communications (ICC2006). Istanbul, 2006. Vol. 3. – P. 1206-1211.

2. Скляр Б. Цифровая связь. М.: Радио и связь, 2000. – 800 с.
3. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М.: Техносфера, 2005. – 320 с.
4. Карташевсий В.Г., Мишин Д.В. Прием кодированных сигналов в каналах с памятью. М.: Радио и связь, 2004. – 239 с.
5. Гладких А.А. Основы теории мягкого декодирования избыточных кодов в стирающем канале связи. Ульяновск: УлГТУ, 2010. – 379 с.
6. Гладких А.А., Мансуров А.И, Черторийский С.Ю. Статистическая оценка индексов достоверности символов, формируемых в системе с мягким декодированием // ИКТ. Т.6, №1, 2008 – С. 39-43.
7. Гладких А.А., Климов Р.В. /Численное моделирование обощенной процедуры формирования индексов мягких решений // ИКТ. Т. 12, № 2, 2013. – С.22-28.
8. Шлома А.М., Бакулин М.Г., Крейнделин В.Б., Шумов А.П. Новые алгоритмы формирования и обработки сигналов в системах подвижной связи. М.: Горячая линия – Телеком, 2008. – 344 с.

METHOD OF FORMATION SOFT SOLUTIONS IN THE SYSTEM BROADBAND COMMUNICATION CHANNEL WITH UNKNOWN PARAMETERS

Baskakova E.S., Gladkikh A.A.

There is resolved the problem of soft-decision symbols indexes forming (SDI) with reference to technology of signal processing with orthogonal frequency division multiplexing (OFDM). The specified technology uses channels with unknown parameters. Such problems are relevant to data exchange between the real-time systems while interaction of two or more mobile objects with wideband communication systems. The SDI calculation is based on Euclidean metrics.

Keywords: *soft-decision decoder, iterative process, erasure, technology OFDM, log-likelihood ratio.*

Баскакова Екатерина Сергеевна, аспирант Кафедры телекоммуникаций (ТК) Ульяновского государственного технического университета (УлГТУ). Тел. 8-917-638-89-63. E-mail: bes_forever87@mail.ru

Гладких Анатолий Афанасьевич, профессор, к.т.н., доцент Кафедры ТК УлГТУ. Тел. 8-842-277-80-82. E-mail: a.gladkikh@ulstu.ru

УДК 621.396.2

ПОМЕХОУСТОЙЧИВОСТЬ СПУТНИКОВОЙ СВЯЗИ ПРИ АКТИВНЫХ ПОМЕХАХ И ОГРАНИЧЕННОЙ ПОЛОСЕ КОГЕРЕНТНОСТИ КАНАЛА

Коротков С.Ю., Пашинцев В.П., Солчатов М.Э., Яремченко С.В.

Разработана методика оценки вероятности ошибочного приема широкополосных сигналов в системах спутниковой связи в условиях возникновения частотно-селективных замираний из-за ограниченной полосы когерентности трансионосферного канала связи и одновременного воздействия узкополосной замирающей активной помехи на вход приемника.

Ключевые слова: вероятность ошибки, спутниковая связь, широкополосный сигнал, трансионосферный канал, частотно-селективные замирания, активная помеха, коэффициент взаимного различия.

Постановка задачи

Известно [1-3], что в системах спутниковой связи (ССС) широкое применение находят сложные широкополосные сигналы (ШПС) с полосой спектра F_0 порядка 1 … 10 МГц. Они обеспечивают уменьшение вероятности ошибочного приема $P_{\text{ош}}$ сигналов оптимальной схемой их обработки на фоне флуктуационных шумов (например некогерентной) при воздействии сосредоточенной по спектру активной помехи (АП). С другой стороны, известно [4-5], что при возмущениях ионосферы на высотах 150 … 400 км слоя F (например путем выброса химических веществ) образуются интенсивные неоднородности, вызывающие многолучевое распространение радиоволн и ограничение полосы когерентности спутникового (трансионосферного) канала связи (КС) до значений $F_{\text{к}} < 100\,\text{кГц}$.

В этих условиях при передаче ШПС с типовыми параметрами:

- полоса спектра $F_0 \approx 2$ … 20 МГц;
- скорость $R_{\text{т}} = 1/T_s = 0,025 \ldots 1,2$ кБод;
- длительность $T_s = 0,04 \ldots 8,3 \cdot 10^{-4}$ с;
- база $B_s = T_s F_0 \approx 1,6 \cdot 10^3 \ldots 4 \cdot 10^5$