

СТАТИСТИЧЕСКАЯ МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ АЛГЕБРАИЧЕСКИХ МЕТОДОВ ОБРАБОТКИ ПСЕВДОСЛУЧАЙНЫХ КОДОВ

С.Г. ВЕКЛИЧ, Т.В. ЛАВРОВСКАЯ, С.Г. РАССОМАХИН

Рассматривается возможность практического применения псевдослучайных кодов в современных системах передачи информации с оценкой их возможного улучшения по параметрам удельной частотной и энергетической эффективности. Построена статистическая модель функционирования системы передачи информации, включающая этапы выбора сообщения источника, генерации псевдослучайного кода, обработки на основе алгебраического метода и декодирования по правилу максимального правдоподобия.

Ключевые слова: псевдослучайный помехоустойчивый код, алгебраические методы обработки, амплитудная модуляция, линейная конгруэнтная генерация, кодовое расстояние.

ВВЕДЕНИЕ

Постановка проблемы. Научно-технический прогресс в области телекоммуникаций в современном обществе предоставляет широкие возможности для информационного обмена. Это является мощным стимулом для развития различных информационных технологий, которые прочно входят в повседневную жизнь. Ведение бизнеса с помощью электронной коммерции, использование Blockchain, применение облачных технологий – вот далеко не полный перечень достижений ИТ области. При этом из года в год возрастает номенклатура и количество технических средств обработки и передачи информации, которые работают в сетях беспроводной связи. Это делает актуальным поиск новых решений рационального использования частотно-энергетического ресурса каналов передачи данных для построения технологий, позволяющих одновременно повысить скорость передачи данных и снизить требуемую мощность передатчиков.

В теории передачи информации известна историческая роль методологии, основанной на использовании случайно выбираемых кодов, в доказательстве фундаментальных теорем для зашумленных каналов [1, 2]. Однако, доказательства на основе случайного выбора кода обычно называются неконструктивными, поскольку до сегодняшнего дня случайные (псевдослучайные) коды (ПСК) для обеспечения помехоустойчивости и конфиденциальности процесса передачи информации не используются. Это является следствием отсутствия приемлемых по вычислительной сложности методов построения и декодирования ПСК, обеспечивающих корректирующую способность, близкую к максимальному правдоподобию. Реализация конструктивных алгоритмов построения и обработки ПСК может быть получена только при

использовании детерминированных алгоритмов генерации псевдослучайных символов кодовых слов.

Привлекательность технологий ПСК заключается в возможности создания сигнально-кодовых конструкций, которые позволяют одновременно повысить как частотную, так и энергетическую эффективность СПИ. Однако основной преградой для широкого использования ПСК в настоящее время является отсутствие не переборных методов декодирования.

Вычислительная сложность алгоритмов, основанных на вычислении евклидовых расстояний возрастает экспоненциально с увеличением длины блока кода и при практически требуемых значениях длины блока является неприемлемой. Получение простых линейных алгебраических методов декодирования наталкивается на трудности, вытекающие из нелинейности детерминированных алгоритмов генерации ПСП. Таким образом, можно утверждать, что идеи применения ПСК могут найти конструктивное воплощение в случае, если будут найдены линейные (линеаризованные) методы декодирования таких кодов.

Цель работы: иллюстрация потенциальных возможностей ПСК на основе исследования статистической модели процесса передачи данных по зашумленным каналам с использованием методов демодуляции, основанных на алгебраических методах.

ОСНОВНАЯ ЧАСТЬ

Рассмотрим обобщенную модель построения блочного псевдослучайного кода. Для получения помехоустойчивого кода поток символов источника, который необходимо передать, разбивается на блоки фиксированной длины по k - бит. При этом каждая комбинация из k двоичных символов источника трактуется, как десятичная количественная величина x_0 – порядковый номер, который определяет даль-

нейшую последовательность псевдослучайных чисел $x_1, x_2, \dots, x_{n-1}$, таким образом x_0 – является числом, порождающим кодовое слово z соответствующим номером. Каждому блоку из k двоичных символов источника ставится в соответствие блок из n недвоичных чисел кода, при этом величина

$$R = \frac{k}{n} \quad (1),$$

является скоростью ПСК и показывает отношение количества информационных двоичных символов сообщения к количеству недвоичных символов кода, предназначенных для передачи по каналу связи. Поскольку длина кодового слова ПСК n , фактически, может выбираться независимо от длины исходного блока двоичных символов k , то скорость кода (1) может быть как больше, так и меньше единицы.

Процесс кодирования состоит в вычислении последовательности символов кодового слова на основе известного порождающего числа x_0 . Получение $(n-1)$ чисел кодового слова на основе числа x_0 осуществляется с применением детерминированной технологии линейной конгруэнтной генерации (ЛКГ) [3]. Свойство линейности этой технологии является принципиальным, поскольку без его выполнения реализация вычислительно простых способов декодирования будет невозможной. Значения числовых символов кодовых слов вычисляются в соответствии со следующими правилами:

$$- x_0 \in [0 \dots (2^k - 1)] - \text{начальный символ} - \text{условный порядковый номер сообщения источника, который порождает кодовое слово};$$

$- x_i = (a \cdot x_{i-1} + b) \bmod m, i \in [1, \dots, (n-1)]$ – числа кодового слова псевдослучайного кода, которые вычисляются по рекуррентному способу, где операция $(A) \bmod m$ – означает вычисление A по модулю m ;

$- a, b$ – константы, m – модуль вычислений;

$- a, b, m$ – целые позитивные числа, которые удовлетворяют условия: $m = 2^k$; b и m – взаимно простые числа, при этом величины $(a-1)$ и m выбираются кратными 4-м.

При выполнении указанных выше условий полученные псевдослучайные целые числа, распределенные равномерно в диапазоне $[0 \dots (2^k - 1)]$, а их последовательность обладает максимальным значением периода повторения. Стоит отметить, что произвольное i -е число последовательности кодового слова связано с начальным порождающим числом x_0 зависимостью:

$$x_i = \left(a^i \cdot x_0 + \frac{a^i - 1}{a - 1} b \right) \bmod m, i \in [1, \dots, n-1]. \quad (2)$$

Рассмотрим наиболее простой способ формирования канальной формы сигналов ПСК на физическом

уровне, основанный на методах амплитудно-фазовой модуляции. Перед процедурой модуляции кодовые слова, являющиеся векторами с десятичными целочисленными координатами, подвергаются преобразованию – центрированию и масштабированию числовых символов. Операция центрирования чисел кодовых слов относительно нуля производится для минимизации необходимой мощности передатчика, при этом исходная последовательность $X = \{x_0, x_1, \dots, x_{m-1}\}$ преобразуется в центрированную последовательность $X' = \{x'_0, x'_1, \dots, x'_{m-1}\}$, где

$$x'_i = x_i - \frac{m-1}{2}, \quad i = 0, 1, \dots, m-1. \quad (3)$$

Числа последовательности X' уже не являются целыми, представляют дискретный ряд с шагом 1 и равномерно распределены в диапазоне $\left[-\frac{m-1}{2}, \frac{m-1}{2}\right]$, абсолютная величина которого равна $\Delta = (m-1)$.

После операции центрирования, координаты полученных векторов X' нормируются в соответствии с выделенным бюджетом энергии на передачу кодового слова. Обозначим E_b – значение средней энергии, которая тратится на передачу одного двоичного символа источника. Тогда для передачи одного символа кода в канале допустимо затратить энергию передатчика, которая определяется выделенным бюджетом и скоростью кода:

$$E_{\text{симв}} = R \cdot E_b, \quad (4)$$

где R – скорость кода, определенная выражением (1).

Числа кодового слова распределены по дискретному равномерному закону, симметрично относительно нуля внутри диапазона Δ . При этом дисперсия D (средняя мощность) сигнала, передающего значение произвольного символа кодового слова определяется дисперсией равномерного распределения и может быть вычислена из выражения

$$D \approx \frac{\Delta^2}{12}. \quad (5)$$

На основании вычисления дисперсии равномерного распределения и введенного ограничения на энергию символа, появляется возможность для определения дополнительных требований к величине нормированного значения Δ^* . Использование выражений (4) и (5) дает:

$$\frac{(\Delta^*)^2}{12} \cdot \tau = R \cdot E_b, \quad \Rightarrow \quad \Delta^* = 2\sqrt{\frac{3}{\tau} \cdot R \cdot E_b}, \quad (6)$$

где τ – продолжительность передачи одного символа кода в канале, которая определяется скоростью модуляции.

Величина Δ^* используется в дальнейшем для нормирования значений псевдослучайных чисел в соответствии с бюджетом выделенной энергии. Процесс нормирования чисел центрированной относи-

тельно нуля последовательности X' состоит в вычислении элементов новой последовательности

$$Z = \{z_0, z_1, \dots, z_{m-1}\}$$

по следующей формуле:

$$z_i = x'_i \cdot \frac{\Delta^*}{\Delta}, \quad i = 0, 1, \dots, n-1. \quad (7)$$

Полученная последовательность чисел

$$Z = \{z_0, z_1, \dots, z_{m-1}\}$$

используется для построения канальной формы составного сигнала, передающего значение кодового слова ПСК. Данный сигнал может быть получен на основе гармонического ортогонального разложения Фурье длительности $n \cdot \tau$:

$$S(t) = \sqrt{\frac{2}{n}} \left\{ \sum_{i=0}^{n-1} z_i \cdot \cos \left[2\pi \left(f_n + \frac{i}{n \cdot \tau} \right) t \right] + \sum_{j=\frac{n}{2}}^{n-1} z_j \cdot \sin \left[2\pi \left(f_n + \frac{j - \frac{n}{2}}{n \cdot \tau} \right) t \right] \right\}, \quad t \in [0, n\tau]. \quad (8)$$

Здесь величина f_n обозначает низшую поднесущую частоту в спектре сигнала для передачи кодового слова; величины $\left(f_n + \frac{i}{n \cdot \tau} \right)$, $\left(f_n + \frac{j - \frac{n}{2}}{n \cdot \tau} \right)$, соответст-

венно, $i(j)$ -е поднесущие частоты; множитель $\sqrt{\frac{2}{n}}$ введен для обеспечения сохранения выделенного бюджета энергии на передачу кодового символа (4), поскольку z_i используется, как амплитуды гармонических колебаний квадратурных компонент, продолжительностью $n \cdot \tau$.

Для примера на рис. 1 показаны отрезки комплексных огибающих сигналов при следующих параметрах псевдослучайного помехоустойчивого кода: $k=10$, $n=5$, $R=2$, $\Delta=31$, $E_b=1$ [Вт·с], $f_n=\frac{1}{5}$ [Гц],

$\tau=1$ [с]. При этом, для генерации кодовых слов по технологии ЛКГ использованы параметры:

$$m=2^k=1024, a=5, b=19.$$

Внешний вид сигналов ПСК напоминает отрезки реализаций случайных процессов. При увеличении длины блока n , спектр огибающих будет расширяться, а их вид приближаться к виду теплового шума.

Стоит отметить, что общий сигнал кодового слова псевдослучайного помехоустойчивого кода предусматривает параллельное кодирование недвоичных символов (чисел) кода, как амплитуд ортогональных на $T=n \cdot \tau$ гармонических поднесущих колебаний.

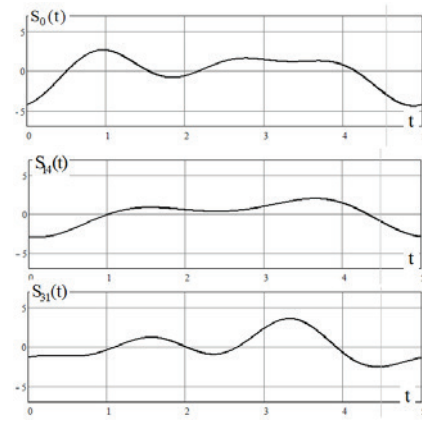


Рис. 1. Примеры комплексных огибающих составных сигналов для разных кодовых слов ПСК

При этом за время T предусматривается параллельная передача n символов кодового слова на квадратурах поднесущих частот.

Рассмотрим процесс цифровой обработки (демоделяции) сигналов кодовых слов ПСК, задаваемых моделью (8) и рис. 1. Данный процесс может быть реализован на основе алгебраических методов. Для этого необходимо произвести дискретизацию сигнала по времени. Минимально необходимое количество независимых измерений сигнала на длительности $n \cdot \tau$ совпадает с длиной кодового слова ПСК n . Моменты проведения измерений распределяются равномерно на отрезке сигнала кодового слова ПСК и определяются величиной T/v , где $v>1$ – константа, значение которой находится из условия достижения наилучшей определенности решаемой в дальнейшем системы линейных алгебраических уравнений (СЛАУ). Моменты дискретных измерений задаются вектором

$$Td = \{td_0, \dots, td_{(n-1)q}\}, \quad (9)$$

где $q \geq 1$ – степень переопределения системы, определяемая отношением числа фактически составленных уравнений СЛАУ к их минимально необходимому количеству n . Компоненты вектора (9) вычисляются из следующего выражения:

$$td_i = \tau \cdot \frac{i}{q \cdot n} \cdot \frac{n}{v}, \quad i = 0, \dots, (n-1)q. \quad (10)$$

Тогда значение сигнала (8) в заданные моменты времени (9) можно записать в виде последовательности дискретных значений

$$S(Td) = \{s(td_0), s(td_1), \dots, s(td_{(n-1)q})\}. \quad (11)$$

Для реализации процесса демодуляции сигнала ПСК используется метод линейной алгебраической обработки сложных сигнальных конструкций. Идея данного метода заключается в определении амплитуд квадратур поднесущих частот сигнала при его известной структуре.

Для этого составляется система линейных алгебраических уравнений вида:

$$A \cdot G = B, \quad (12)$$

где A – матрица коэффициентов квадратурных компонент на интервале модуляции; B – вектор значений сигнала в цифровом представлении в каждый момент времени; G – вектор искоемых значений амплитуд для заданного интервала модуляции.

В общем случае для решения системы (12) наиболее выгодным с точки зрения максимального учета информации о сигнале является решение переопределенной СЛАУ $N > n$, где $N = n \cdot q$. Для формирования переопределенной СЛАУ используются дополнительные измерения сигнала из выборки (11), содержащей большее количество уравнений при том же самом количестве неизвестных.

Размерность прямоугольной матрицы A определяется как $(N \times n)$. Система (12) при наилучшем значении v является совместной, хорошо определенной, что обеспечивает существование единственного решения. Для решения СЛАУ на произвольном i -м интервале модуляции при передаче n -символьного кодового слова ПСК следует выбрать $(n \cdot q)$ равномерно расположенных отсчетов массива измерений выборки, начиная с позиции начала наблюдения полного тактового интервала сигнала. Матрица коэффициентов при искоемых значениях амплитуд квадратурных колебаний A и матрица-столбец свободных членов уравнений B формируется, с использованием максимального количества измерений на интервале модуляции длительностью T :

$$A = \|a_{i,j}\|, \quad i = 0, \dots, (n-1) \cdot q, \quad j = 0, \dots, (n-1);$$

$$a_{i,j} = \sqrt{\frac{2}{n}} \cdot \cos \left[2\pi \left(f_n + \frac{j}{n \cdot \tau} \right) t_i \right], \quad 0 \leq j \leq \left(\frac{n}{2} - 1 \right); \quad (13)$$

$$a_{i,j} = \sqrt{\frac{2}{n}} \cdot \sin \left[2\pi \left(f_n + \frac{j - \frac{n}{2}}{n \cdot \tau} \right) t_i \right], \quad \frac{n}{2} \leq j \leq (n-1).$$

Матрица-столбец свободных членов формируется в виде вектора измерений сигнала на длительности одного интервала модуляции:

$$B = S(Td), \quad b_i = s(td_i), \quad (14)$$

где $i = 0, \dots, (n-1) \cdot q$.

Система (12) имеет множество способов получения точных или приближенных решений. На практике наиболее часто используют метод на основе правила наименьших квадратов, приводящий к оценке вида:

$$G = (A^T \cdot A)^{-1} A^T \cdot B. \quad (15)$$

Решение системы (15) является приближенным, но, в условиях помеховых искажений и шума квантования при измерениях, результат получается более точным, чем при решении строгой (не переопределенной) системы (12). Помехоустойчивость решения достигается путем усреднения действия помех при

числе измерений сигнала, превышающим минимальное необходимое [4].

Дальнейшая обработка вектора G позволяет определить номер полученного сигнала. Определение номера принятого сигнала заключается в нахождении номера минимального по абсолютной величине неотрицательного элемента вектора

$$Z' = \{z'_0, z'_1, \dots, z'_{m-1}\}.$$

Элементы данного вектора поочередно вычисляются, как евклидово расстояние между наблюдаемым на выходе канала вектором и всеми возможными векторами кодовой книги ПСК:

$$z'_c = |G - z_c|, \quad c = 0, \dots, (m-1). \quad (13)$$

Критерий максимального правдоподобия при приеме кодового слова с номером i имеет вид:

$$X^* = X_i \text{ if } z'_i = \min_{i \in 0 \dots (m-1)} \{Z'\}. \quad (14)$$

Для статистической оценки помехоустойчивости систем передачи информации, использующих псевдослучайные коды рассмотренной выше конструкции, разработаны статистические модели приема сигналов в условиях отсутствия помех и в условиях зашумленного канала. Схема алгоритма работы статистической модели системы с псевдослучайным кодированием в условиях отсутствия помех (действует только шум квантования) представлена на рисунке 2.

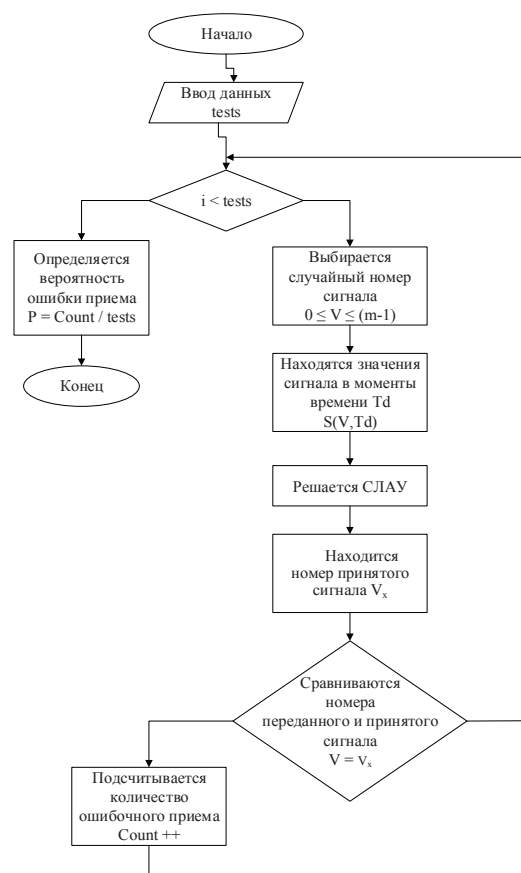


Рис. 2. Блок-схема алгоритма статистической модели обработки ПСК в условиях отсутствия помех

В модели проводится серия из tests испытаний, каждое из которых предполагает случайный выбор произвольного кодового слова, формирование канальной формы составного сигнала ПСК в соответствии с правилом (8), решение СЛАУ демодуляции (13) – (15) и принятие решения по критерию (14) на основе вычисления элементов кортежа взаимных расстояний (13). По результатам испытаний производится оценка вероятности возникновения ошибок при декодировании. Данная модель предназначена для проверки робастности алгоритмов формирования и алгебраической обработки отрезков псевдослучайных последовательностей, которые соответствуют кодовым словам ПСК.

Исследование помехоустойчивости разработанных конструкций ПСК в условиях действия аддитивного гауссова шума с плоским спектром проведено на основе статистической модели, схема алгоритма которой представлена на рисунке 3.

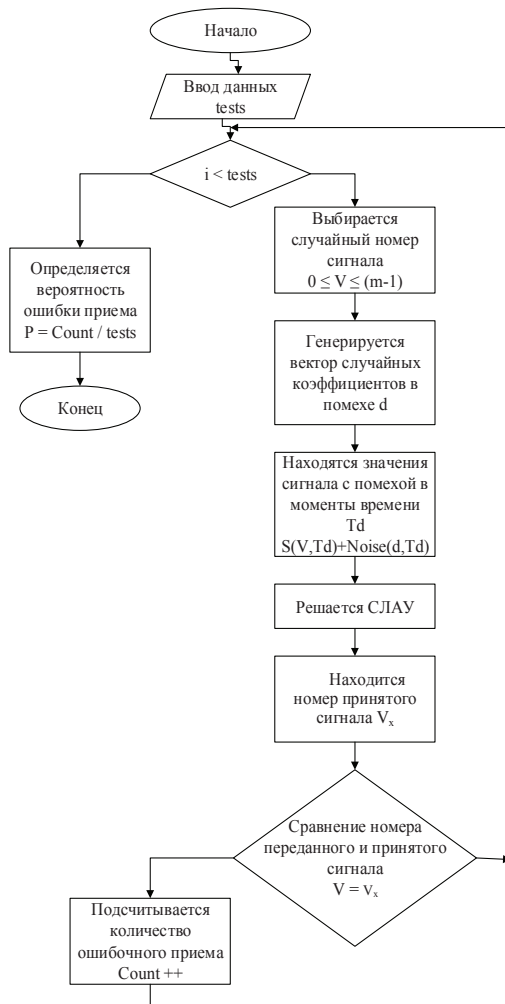


Рис. 3. Блок-схема алгоритма статистической модели для испытаний ПСК в условиях действия гауссовой аддитивной помехи

Аналитическая модель реализации помехи в данной модели имеет следующий вид:

$$\text{Noise}(t) = \sqrt{\frac{1}{n}} \left\{ \sum_{i=0}^{n-1} d_i \cdot \cos \left[2\pi \left(f_n + \frac{i}{n \cdot \tau} \right) t \right] + \sum_{j=\frac{n}{2}}^{n-1} d_j \cdot \sin \left[2\pi \left(f_n + \frac{j - \frac{n}{2}}{n \cdot \tau} \right) t \right] \right\}, \quad t \in [0, T], \quad (15)$$

где номенклатура поднесущих квадратур совпадает с соответствующей номенклатурой, использованной при построении канальной формы составного сигнала ПСК (8); d – n -мерный вектор с нормально распределенными координатами, обладающими нулевым математическим ожиданием и дисперсией N_0/n . Величина N_0 равна спектральной плотности мощности аддитивной гауссовой помехи. Использованная методика нормировки мощности сигнала (4) – (7) позволяет определить величину отношения сигнал/шум, приведенную к одному передаваемому двоичному символу сообщения источника, в виде:

$$S/N = (N_0)^{-1}. \quad (16)$$

Принимаемый сигнал в данной модели является продуктом аддитивного взаимодействия:

$$S_N(t) = S(t) + \text{Noise}(t). \quad (17)$$

Отличие алгоритма статистических испытаний в зашумленном канале (рис. 3) от рассмотренного ранее заключается в добавлении реализации помехи со структурой, определяемой (15) перед осуществлением алгебраической обработки аддитивной смеси, наблюдаемой на выходе гауссова канала. При этом в модели, кроме задания параметров ПСК скорости R и длины блока n , предусмотрена возможность регулирования величины отношения сигнал/шум путем изменения величины спектральной плотности мощности помехи N_0 .

Статистическая модель позволяет исследовать помехоустойчивость конструкций ПСК при действии помех в канале, а также оценить эффективность алгебраических методов обработки при демодуляции. Результаты статистических испытаний моделей формирования и алгебраической обработки ПСК при наличии аддитивного гауссова шума представлены на рисунках 4 – 6.

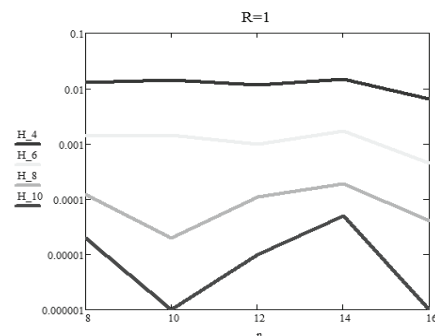


Рис. 4. Зависимости вероятности ошибки приема кодового слова ПСК от длины блока ПСК n при различных значениях отношения сигнал/шум H и $R=1$

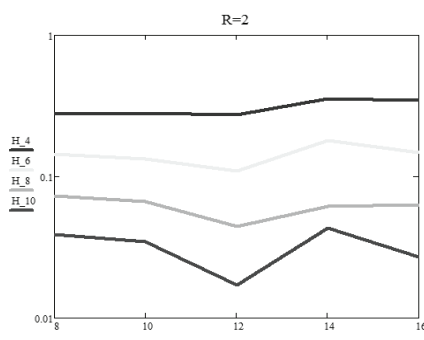


Рис. 5. Зависимости вероятности ошибки приема кодового слова ПСК от длины блока ПСК n при различных значениях отношения сигнал/шум H и $R=2$

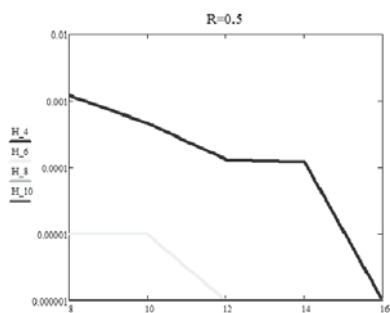


Рис. 6. Зависимости вероятности ошибки приема кодового слова ПСК от длины блока ПСК n при различных значениях отношения сигнал/шум H и $R=0,5$

ЗАКЛЮЧЕНИЕ

Полученные результаты статистического исследования моделей функционирования СПИ при использовании алгебраических методов демодуляции и применении декодирования псевдослучайных кодов ЛКГ по правилу максимального правдоподобия показывают, что, практически, при любых скоростях кода R , не превышающих пропускную способность гауссова канала, простое увеличение длины блока кодовых слов позволяет добиться сколь угодно малой величины вероятности декодирования с ошибкой. Применение ПСК в сочетании с алгебраической демодуляцией псевдошумовых последовательностей снижает вычислительную сложность задачи обработки рассмотренных сигнально-кодовых конструкций. Это позволяет констатировать перспективность рассмотренных технологий для реализации в современных высокоскоростных системах передачи информации.

Литература

- [1] Shannon C. E., A Mathematical Theory of Communication / Shannon C. E. // Bell Syst. Tech. J., July-Oct. 1948. – Vol. 27. – P. 379 – 423, 623 – 656.
- [2] Shannon C.E. Communication in the presence of noise / Shannon C.E. // Proc. IRE., Jan. 1949. – Vol. 37. – P. 10 – 21.
- [3] Лавровская, Т.В. Физическая модель псевдослучайных кодов в многомерном Евклидовом пространстве/ Т.В. Лавровская, С.Г. Рассомахин // Системи озброєння і військова техніка. – 2016. – Вып. 3 (47). – С. 79-84

- [4] Веклич С.Г. Линейная алгебраическая обработка сложных сигнальных конструкций / С.Г. Веклич, С.Г. Рассомахин // Системи обробки інформації. – 2016. – Вып. 8 (145). – С. 40 – 43



Веклич Сергей Геннадиевич, аспирант кафедры БИСТ ХНУ имени В. Н. Каразина. Научные интересы: Информационная безопасность, теория передачи информации.



Лавровская Тамила Валериевна, аспирант кафедры БИСТ ХНУ имени В. Н. Каразина. Научные интересы: Информационная безопасность, теория передачи информации.



Рассомахин Сергей Геннадиевич, доктор технической наук, доцент, заведующий кафедрой БИСТ ХНУ им. В.Н. Каразина. Научные интересы: Информационная безопасность, теория передачи информации.

УДК 621.37:621.391

Статистична модель функціонування системи передачі інформації при використанні алгебраїчних методів обробки псевдовипадкових кодів / С.Г. Веклич, Т.В. Лавровська, С.Г. Рассомахин // Прикладна радіоелектроніка: наук.-техн. журнал. – 2016. – Том 15, № 3. – С. 226 – 231.

Розглядається можливість практичного застосування псевдовипадкових кодів у сучасних системах передачі інформації з оцінкою їх, можливого, поліпшення за параметрами питомої частотної та енергетичної ефективності. Побудована статистична модель функціонування системи передачі інформації, що включає етапи вибору повідомлення джерела, генерації псевдовипадкового коду, обробки на основі алгебраїчного методу і декодування за правилом максимальної правдоподібності.

Ключові слова: псевдовипадковий завадостійкий код, алгебраїчні методи обробки, амплітудна модуляція, лінійна конгруентна генерація, кодова відстань.

Ил.: 06. Библиогр.: 04 назв.

UDC 621.37:621.391

Statistical model of functioning an information transmission system using algebraic methods of processing pseudorandom codes / S.G. Veklych, T.V. Lavrovskaya, S.G. Rassomakhin // Applied Radio Electronics: Sci. Journ. – 2016. – Vol. 15, № 3. – P. 226 – 231.

The possibility of practical application of pseudorandom codes in modern information transmission systems with assessment of their possible improving in parameters of specific frequency and energetic efficiency is considered. A statistical model of functioning an information transmission system is constructed which includes stages of choosing of the message of a source, pseudorandom code generations, processing on the basis of an algebraic method and decoding by the rule of maximum likelihood.

Keywords: interference pseudorandom code, algebraic processing methods, amplitude modulation, linear congruent generation, code distance.

Fig.: 06. Ref.: 04 items.