$$X_i = \Phi X_{i-1} + \Gamma m_{i-1}, \qquad (11)$$

где Φ и Γ – матрицы перехода системы и возмущающего воздействия из (i-1)-го в i-е состояние.

Основной составляющей вектора x_i, получившего общее название вектора состояния, является вектор параметров движения ВС. Объединяя уравнение состояния с уравнением наблюдений $U = HX + \omega$, отражающим связь между отклонениями измеренных U и определяемых X величин от своих счислимых значений с учётом погрешностей измерений ω, получают полную систему уравнений, фильтра Кальмана. Эти уравнения позволяют описывать сложные нестационарные процессы в любых динамических системах, в том числе и в системах навигации.

Из рассмотренных алгоритмов видны особенности процесса динамической фильтрации и его отличие от процесса статистической обработки данных, осуществляемого по методу наименьших квадратов.

Очевидно, что в процессе динамической фильтрации учитываются измерения параметров движения от измерения к измерению, обусловленные внешними воздействиями на ВС, а также дополнительный случайный разброс значений параметров движения из-за этих возмущений. Таким образом, с помощью алгоритмов динамической фильтрации осуществляется более полное адекватное описание процессов, протекающих в бортовом навигационном комплексе ВС.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Глухов В.В.* Техническое диагностирование динамических систем.– М.:Транспорт. 2000.– 95 с.

2. *Белявский Л.С., Новиков В.С., Олянюк П.В.* Основы радионавигации./ Под. ред. Л.С. Белявского. – М.:Транспорт, 1992.– 320 с.

3. *Исмаилов И.М.* Эффективность использования полетной информации для контроля управления движением воздушного судна.- Вопросы специальной радиоэлектроники. Научно-технический сборник. Серия общие вопросы радиоэлектроники. Выпуск 3. – Москва – Таганрог, 2006.

А.П. Жук, И.В. Галкин, В.В. Сазонов, З.В. Черняк, Е.В. Топкин
Россия, г. Ставрополь, СВИС РВ

ОЦЕНКА СТРУКТУРНОЙ СКРЫТНОСТИ СИГНАЛОВ В СИСТЕМЕ ПЕРЕДАЧИ ИНФОРМАЦИИ С ОРТОГОНАЛЬНЫМИ ПОСЛЕДОВАТЕЛЬНОСТЯМИ

Структурная скрытность характеризует способность противостоять мерам радиотехнической разведки, направленным на раскрытие структуры сигнала. Это означает распознавание формы сигнала, определяемой способами его кодирования и модуляции, т.е. отождествление обнаруженного сигнала с одним из множества априорно известных.

Следовательно, для увеличения структурной скрытности необходимо иметь по возможности больший ансамбль используемых сигналов и достаточно часто изменять форму сигналов [6].

Это возможно за счет стохастического использования ансамблей дискретных ортогональных многоуровневых сигналов (АДОМС), описываемых собственными векторами бидиагональной симметрических матриц (БСМ) [2,3].

Известно [4], что при бесконечно большом наборе коэффициентов диагональных симметрических матриц {N} существует бесконечно большое число ортогональных базисов {M}. К этому заключению приводит ряд теорем теории матриц. Дискретный сигнал x(t) однозначно определяется вектором в N-мерном пространстве:

$$\vec{x} = (x_1; x_2; \ldots; x_N),$$

где $x_i = x(t)$ при $t \in [(i-1)\Delta t; i\Delta t]$.

В этом пространстве имеется N-мерный ортогональный базис, и каждой оси базиса соответствует определенный элемент дискретного сигнала, амплитуда которого определяет координату сигнального вектора по данной оси, поэтому ансамбль дискретных ортогональных сигналов задает система функций

$$\{x_1(t); x_2(t); \ldots x_n(t)\}.$$

На общем минимальном отрезке Δt каждый сигнал моделируется точкой арифметического N-мерного пространства R^N, которое рассматривается как частный случай линейного пространства матриц, а ансамбль сигналов однозначно определяется матрицей порядка $n \times N$:

$$|x_{ik}| = \begin{bmatrix} x_{11} & x_{12} & \ldots & x_{1N} \\ x_{21} & x_{22} & \ldots & x_{2N} \\ \ldots & \ldots & \ldots & \ldots \\ x_{n1} & x_{n2} & \ldots & x_{nN} \end{bmatrix}, \tag{1}$$

где $x_{ik} = x_i(t); i = 1,2,3,\ldots,n$, при $t \in [(k-1)\Delta t; k\Delta t]$.

Матрица, определяемая согласно (1), является моделью ансамбля дискретных сигналов. Для каждой симметрической матрицы существует, по крайней мере, один действительный или комплексный собственный вектор, координаты которого являются решением характеристического уравнения n-й степени. Корни этого характеристического уравнения называются собственными значениями матрицы А. При этом собственные векторы $\vec{x}$ и $\vec{y}$ симметрической матрицы А, соответствующие собственным значениям λ и μ, удовлетворяют условию ортогональности [5]:

$$\vec{x} \cdot \vec{y} = 0.$$

Множество матриц А порядка ($n \times n$), все элементы которых целые числа, задают все возможные базисы пространства E_n.

А пространство моделей ансамблей дискретных ортогональных сигналов состоит из множества базисов, соответствующих различным действительным симметрическим матрицам [2,5].

Целью статьи является оценка влияния размерности, диапазона и шага изменения коэффициентов БСМ на структурную скрытность модифицированного способа защиты информации со стохастическим применением АДОМС.

В защищенной системе передачи с ортогональными сигналами [2,3 каждая уникальная симметрическая матрица соответствует уникальному базису ДОС, поэтому размерность множества различных матриц равна размерности множества таблиц *H*.

Математически формирование случайной таблицы *H* выполняется в два этапа. На первом этапе – строится базис, соответствующий случайно заполненной БСМ размерности *N*, по вторым диагоналям.

Для этого используется *N*-1 случайно выбранный коэффициент некоторого диапазона [-*a*, *a*] с точностью до порядка Δ. Затем выполняется случайная перестановка в таблице ранее записанных векторов.

Множество всех действительных симметрических матриц (*n*) равно количеству перемещений с повторением A_k^r из k элементов по r. Число различных размещений с повторениями [1]:

$$n = A_k^r = k^r,$$

которое, в данном случае, определяется следующим образом:

$$n = 1 + \frac{|-a| + |a|}{\Delta} = 1 + \frac{2a}{\Delta}, \text{ а } r = N\text{-}1.$$

Следовательно, множество всех симметрических матриц (n) равно

$$n = \left(1 + \frac{2a}{\Delta}\right)^{N-1}. \qquad (2)$$

Случайное «взбивание» таблицы *H* позволяет получить множество случайных таблиц, количество элементов которых равно количеству перестановок P_N из *N* элементов, т.е.

$$m = P_N = N!. \qquad (3)$$

Анализ соотношений (2) и (3) позволяет сделать вывод, что размерность ключевого пространства (*Z*) для данного способа защиты вычисляется по формуле

$$Z = m \cdot n = \left(1 + \frac{2a}{\Delta}\right)^{N-1} \cdot N!.$$

Следовательно, вероятность раскрытия структуры сигнала в защищённом канале связи в этом случае равна

$$P_{рас.} = \frac{1}{\left(1 + \frac{2a}{\Delta}\right)^{N-1} \cdot N!}.$$

Проведем оценку вероятности раскрытия структуры сигнала от величины границы промежутка и размерности БСМ. Очевидно, что с увеличением величины диапазона [-*a*, *a*] при равных остальных условиях, а именно заданной точности и неизменной размерности БСМ, вероятность раскрытия структуры сигнала в защищённом канале связи будет уменьшаться.

Данная зависимость наглядно представлена на графике, изображенном на рис. 1, при *N*=1, Δ=0,1.

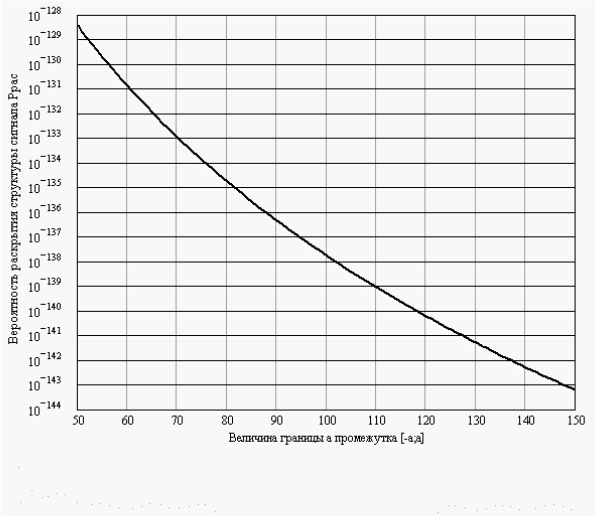

Рис. 1. Зависимость вероятности раскрытия структуры сигнала $P_{рас}$ от величины диапазона [-a, a]

Из анализа графика, представленного на рис. 1, следует, что бесконечно увеличивать диапазон [-*a*, *a*] не имеет смысла, т.к. выигрыш от увеличения вероятности раскрытия в данном случае будет меньше по сравнению со сложностями, возникшими при физической реализации устройств передачи и приёма информации.

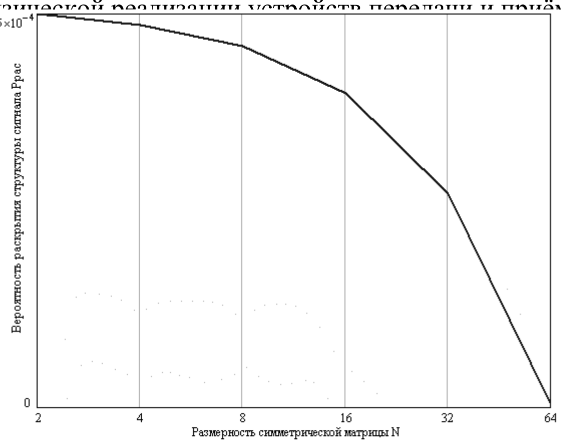

Рис. 2 Зависимость вероятности раскрытия структуры сигнала $P_{рас}$ от размерности симметрической матрицы N

Далее определим зависимость вероятности раскрытия $P_{рас}$ от размерности *N* БСМ. Данная зависимость наглядно представлена на рис. 2, при a=100, Δ=0,1.

Откуда следует что с увеличением размерности симметрической матрицы, вероятность раскрытия значительно уменьшается.

По мнению авторов, применение АДОМС с изменяемой размерностью в системе передачи информации позволяет достичь требуемого уровня структурной скрытности передаваемой информации.

Подводя итог вышеизложенному, можно сказать, что структурная скрытность модифицированного способа защиты информации со стохастическим применением АДОМС, построенных на основе свойств собственных векторов БСМ, напрямую зависит от ее размерности, диапазона и шага изменения коэффициентов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Гмурман В.Е.* Теория вероятностей и математическая статистика. Учеб. пособие для вузов. Изд. 7-е, стер. – М.: Высш. шк., 2001.

2. *Жук А.П., Жук Е.П.* Способ повышения помехозащищенности систем связи с ортогональными сигналами //Инфокоммуникационные технологии. Том 3. №4. 2005. – Самара, 2005.

3. *Жук А.П., Марченко Е.А.* Повышение скрытности систем связи с ортогональными сигналами. Сборник научных трудов Ставропольского ВИС РВ. Выпуск 23. – Ставрополь: СВИС РВ, 2005.

4. *Парлетт Б.* Симметричная проблема собственных значений/Пер. с англ. – М.: Мир, 1983.

5. *Попенко В.С.* Векторный синтез ансамблей ортогональных сигналов. Ч.II. – МО, РФ, 1993.

6. Помехозащищенность радиосистем со сложными сигналами Под ред. Г.И. Тузова. – М.: Радио и связь, 1985.

А.П. Жук, В.В. Сазонов, С.И. Авдеенко
Россия, г. Ставрополь, СВИС РВ

АЛГОРИТМ ПОСТРОЕНИЯ ТРЕБУЕМОЙ ФАЗОВОЙ СТРУКТУРЫ АНСАМБЛЯ ДИСКРЕТНЫХ ОРТОГОНАЛЬНЫХ В УСИЛЕННОМ СМЫСЛЕ СИГНАЛОВ

В работах [2,3] доказано, что для всякого ортогонального базиса конечномерного комплексного пространства существует эрмитова матрица (ЭМ) Q самосопряженного оператора, собственные векторы которой составляют данный базис. Координаты собственных векторов эрмитовой матрицы в общем случае являются комплексными числами, а условие ортогональности в комплексном пространстве совпадает с условием ортогональности в усиленном смысле, представленным для дискретных аналитических комплексно-сопряжённых сигналов $\dot{x}(t)$ и $\dot{y}^*(t)$ [1]:

$$\int_0^T \dot{x}(t)\dot{y}^*(t)dt = 0, \tag{1}$$

где $\dot{x}(t)=a(t)\cdot e^{j\psi_i(t)}$, $\dot{y}^* = b(t)\cdot e^{j\psi_j^*(t)}$, причем $a(t)=b(t)$ - амплитуды сигналов, а $\psi_i(t)$ и $\psi_j^*(t)$ соответственно фазы сигналов, причём вторая комплексно сопряжена.

Однако предложенная в [3] методика обладает недостатками, связанными прежде всего, со сложными аналитическими зависимостями фазовой $\psi(t)$ структуры синтезированных ансамблей дискретных ортогональных в усиленном смысле сигналов (АДОУСС) и коэффициентами второй диагонали ЭМ. Это требует существенных временных затрат при синтезе ансамблей с объёмом алфавита $m > 8$.