IST '10

24-25 ноября
2010 года
Минск, Беларусь

Материалы VI Международной конференции

Информационные системы и технологии

IST'2010

Informational systems and technologies

INFOPARK

АНАЛИЗ ИНСТРУМЕНТАЛЬНЫХ МЕТОДОВ ОЦЕНКИ ЗАЩИЩЕННОСТИ ЦИФРОВЫХ КАНАЛОВ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ

Д.С. Рябенко, В.К. Железняк

Полоцкий государственный университет, кафедра технологий программирования
г. Новополоцк, ул. Блохина 29, +375 214 53-53-56,
e-mail: denis-kurs@rambler.ru

Защита цифровых систем передачи речевой информации от утечки по техническим каналам является актуальной научной и технической задачей. Защита информации устанавливается, исходя из модели информационного объекта.

В работе рассматриваются речевые системы, основанные на кодировании мгновенных значений речевого сигнала или его приращений. Принцип систем состоит в том, что сигнал или его приращения дискретизируются, а значения отсчета каждого шага дискретизации на передающей стороне кодируются бинарным кодом. Последовательность кодовых групп передается на приемную сторону для приема и декодирования и восстановления исходной формы речевого сигнала.

Количественной мерой помехоустойчивости является степень соответствия принятого сообщения переданному, т.е. точность воспроизведения.

Для аналоговых систем мерой качества является отношение сигнал/шум $S_c/N = \sigma_c^2/\sigma_ш^2$ либо среднеквадратическая ошибка передаваемого сигнала $E\left[\left(S_c - \hat{S}_c\right)^2\right]$.

В отличие от аналоговых меру качества передачи информации цифровыми системами оценивают вероятностью правильного решения (определения) переданных символов на выходе приемника.

Оптимальный приемник реализуют для когерентного либо некогерентного приема по схеме согласованных фильтров либо корреляционного приемника для априори заданного сигнала.

Расчет помехоустойчивости единичных символов при оптимальном приеме полностью известных двоичных символов, передаваемых по каналу с постоянными параметрами и аддитивной помехой в виде белого гауссового шума, представлен формулой [1]

$$P_0 = 0{,}5\left(1 - \Phi\left[\left(E_1 + E_0 - \rho\sqrt{E_1 E_0}\right) \Big/ 2N_0\right]\right), \quad (1.1)$$

где E_1 и E_0 – энергия единичных сигналов $S_1(t)$ и $S_0(t)$;

P_0 – вероятность ошибки приема символа;

ρ – коэффициент корреляции между сигналами $S_1(t)$ и $S_0(t)$;

N_0 – спектральная плотность мощности шума;

$\Phi(x)$ – табулированная функция Крампа [2].

Для сигналов равных энергий при использовании амплитудной, частотной (ортогональных сигналов) и фазовой манипуляции вероятности ошибки зависят от параметра $h^2 = \frac{E_c}{N_0}$ [2].

Максимальной потенциальной помехоустойчивостью обладает фазомодулированный сигнал, т.е. является оптимальной системой. Потенциальная помехоустойчивость реализуется при когерентном приеме и согласовании параметра тракта со структурой и параметрами сигнала.

Канал утечки информации характеризуется слабым сигналом, шумами высокого уровня, согласование его характеристик с параметрами сигнала не обеспечивается. Фаза сигнала, поступающего из канала утечки, на входе приемника случайная по гармонической несущей, а по огибающей сигнала принято считать когерентной [3].

Для многократной ФМ с m_c позициями вероятность ошибочной регистрации $P_{0ФМ}$ определяется выражением

$$P_{0ФМ} = \left(1 \Big/ \log_2 m_c\right)\left[1 - \Phi\left(\sqrt{2}q \sin \pi / m_c\right)\right] \quad (1.2)$$

Схема оптимального обнаружителя представлена на рис. 1. Она вычисляет корреляционный интеграл, сравнивает его с порогом и выдает решение A с вероятностями P_0, P_1 [3]:

$$z(T) = \int_0^T x(t)u(t)dt. \quad (1.3)$$

При вычислении корреляционного интеграла $z(T)$ осуществляется переход от многомерного распределения n выборочных значений напряжения на входе обнаружителя к одномерному распределению напряжения $z(T)$ на его выходе в момент времени T в результате

накопления (суммирования) n выборочных значений в течение длительности выборки T.

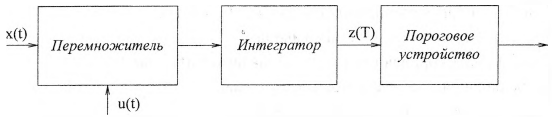

Рис. 1. Схема оптимального обнаружителя

Если входная выборка представляет собой шум n, то $z_n(T)$ определяет напряжение шума на выходе коррелятора. Если выборка — смесь сигнала с шумом, то z_{nc} (T) можно рассматривать на выходе как аддитивную смесь, поскольку операции суммирования и интегрирования линейные.

Переход от суммы выборочных значений при $n \to \infty$ и T = const к интегралу осуществляется на основании теоремы Котельникова. Напряжение шума на выходе коррелятора

$$z_n(T) = \int_0^T n(t)u(t)dt. \tag{1.4}$$

Напряжение смеси

$$z_{nc}(T) = \int_0^T [x(t) + n(t)]u(t)dt.$$

Эти напряжения есть максимальные значения отклика коррелятора на шум и смесь соответственно. Превышение порога z_0 происходит с вероятностями, отличными от единицы. Превышение порога z_0 — величиной z_{nc} (T) есть правильное обнаружение и вероятность превышения называется вероятностью правильного обнаружения P_0, а превышение порога z_0 величиной z_n (T) с вероятностью $P_л$ называется ложной тревогой.

Отношение правдоподобия для сигнала со случайной фазой

$$\bar{l}(x) = \left[\exp\left(-E/N_0\right)\right] I_0\left[2Z(T)/N_0\right]. \tag{1.5}$$

Показатель экспоненты является постоянной величиной, $l(x)$ — монотонной функцией $Z(T)$, поэтому оптимальным правилом решения

задачи обнаружения сигнала является вычисление корреляционного интеграла Z(*T*). Затем Z (T) сравнивается с порогом Z_0.

Если Z (T) > Z_0 — сигнал есть,

если Z (T) <; Z_0 — сигнала нет.

Структурная схема оптимального обнаружителя сигнала со случайной начальной фазой представлена на рис. 2 [4]. В каждом канале вычисляется корреляционный интеграл z_1 (T) и z_2 (T) соответственно. В квадратичном детекторе осуществляется операция возведения в квадрат; после вычисления величины $z^2 = (z_1^2 + z_2^2)$ производится вычисление логарифма функции Бесселя от аргумента, пропорционального модулю корреляционного интеграла, и сравнение его в пороговом устройстве с пороговым значением Z_0= ln I_0+ (E/G_0). В качестве опорных напряжений на умножителях используются сдвинутые по фазе на π/2 колебания высокой или промежуточной частоты $u_1=u(t)cos[w_0t-\psi(t)]$ и $u_2=u(t)sin[w_0t+\psi(t)]$. Наличие двух квадратурных каналом позволяет исключить зависимость значения отношении правдоподобия от начальной фазы полезного сигнала.

Значение порогового уровня Z_0 может быть определяется решением относительно Z трансцендентного уравнения

$$I_0 (2Z/G_0) = I_0 \exp (E/G_0).$$

Для вычисления характеристик обнаружения необходимо определить условные плотности вероятности модуля корреляционного интеграла при условиях наличия и отсутствия полезного сигнала во входной смеси.

Рис. 2 Структурная схема оптимального обнаружителя сигнала со случайной начальной фазой.

При указанных условиях распределение модуля корреляционного интеграла при отсутствии сигнала (A=0) подчинено закону Рэлея, а при наличии сигнала (A=1) определяется законом Раиса [4]:

$$p(Z \mid A_0) = \frac{2Z}{G_0 E} \exp\left(-\frac{Z^2}{G_0 E}\right);$$
$$p(Z \mid A_1) = \frac{2Z}{G_0 E} \exp\left(-\frac{Z^2 + E^2}{G_0 E}\right) I_0\left(\frac{2Z}{G_0}\right). \qquad (1.9)$$

ЛИТЕРАТУРА

1. Чернега, А.С. Расчет и проектирование технических средств обмена и передачи информации / А.С. Чернега, В.А. Василенко, В.Н. Бондарев // Учеб. пособие для вузов. – М.: Высшая школа. 1990. – 224с.
2. Лахти, Б.П. Система передачи информации / Б.П. Лахти; пер с англ. под общей ред. Б.П. Кувшинова. – М.: Связь. 1971. – 324с.
3. Стифлер, Дж. Теория синхронной связи / Дж. Стифлер, пер. с англ. Б.С.Цыбакова; под ред. Э.М.Габидулина. – М.: Связь; 1975. – 488с.
4. Охонский, А.Г. Помехоустойчивость информации радиосигналов управления / А.Г. Охонский, А.А. Елисеев, Н.В. Каплунова, А.Н. Кулин, Э.В. Минько; под. ред. А.Г. Охонского // Учеб. Пособие – М.: изд-во МКАП "Мир книги", 1993. 216с.