

# ИНФОРМАЦИОННЫЕ ПОКАЗАТЕЛИ, ГАРАНТИРУЮЩИЕ ЗАЩИЩЕННОСТЬ ЦИФРОВОЙ РЕЧИ

В.К. Железняк, Д.С. Рябенко

Полоцкий государственный университет, научно-исследовательская  
опытно-экспериментальная лаборатория технической защиты информации  
211440, ул. Блохина 29, Новополоцк, Беларусь  
телефон: 8 (0214) 535356; факс: 8 (0214) 534263; e-mail: Vlad@psu.by

Целью работы является установление и обоснование критерия защищенности цифровых речевых сигналов и определение его зависимости от критерия (нормированного показателя) защиты аналогового речевого сигнала.

Защищенность цифровых речевых сигналов, пропускная способность, энергетическая и частотная эффективность систем передачи.

Передача сигналов, преобразованных в цифровую форму, обладает несомненными преимуществами перед передачей аналоговых сигналов. Благодаря наиболее совершенным достижениям предельного качества и высокого уровня достоверности передачи цифровых данных усложнились способы защиты от утечки информации.

Речевой сигнал воспринимается человеком только в аналоговой форме. Первичный, цифровой и преобразованный из цифрового сигнала в аналоговую форму речевой сигнал должны быть защищены от утечки информации по техническим каналам.

Защищенность аналоговых сигналов оценивают по научно-обоснованному критерию (нормативному показателю).

Для исследований выбрана модель двоичного симметричного канала (ДСК). В системах с многопозиционными сигналами существуют аналогичные зависимости.

Предельные значения показателей эффективности достигаются при  $R = C$  и определяются следующими выражениями [1]:

$$\gamma_N = C_N, \quad \beta_N = C_N / E_N / N_0 \quad (1.1)$$

Основной характеристикой ДСК является вероятность ошибки  $P$ .

$$P = Q(\sqrt{2 \cdot E_s / N_0}), \quad (1.2)$$

где  $E_s$  – энергия бита,  $N_0$  – спектральная плотность шума,  $Q(x)$  – функция, определяемая по формуле

$$Q(x) = 1/2\pi \cdot \int_x^\infty e^{-t^2/2} dt. \quad (1.3)$$

Пропускная способность ДСК  $C$  определяется по формуле [1, 2]:

$$R_{\max} = C = W[1 + P \log_2 P + (1 - P) \log_2 (1 - P)]. \quad (1.4)$$

Из формулы (1.4) следует, что  $C$  прямо пропорционально зависит от  $W$ , а также от  $P$ . Пропускная способность  $C$  стремится к 0 с увеличением  $P$  до 0,5.

Зависимость вычислительной скорости  $R_0$  от вероятности ошибки рассмотрена в [3].

Рассмотрены зависимость  $E_s/N_0$  от  $P$  в зависимости от сигналов [4]:

сигналы противофазные

$$P = Q(-\sqrt{2 \cdot E_s / N_0}); \quad (1.5)$$

сигналы ортогональные

$$P = Q(-\sqrt{E_s / N_0}); \quad (1.6)$$

сигналы с пассивной паузой

$$P = Q(-\sqrt{1/2 \cdot E_s / N_0}). \quad (1.7)$$

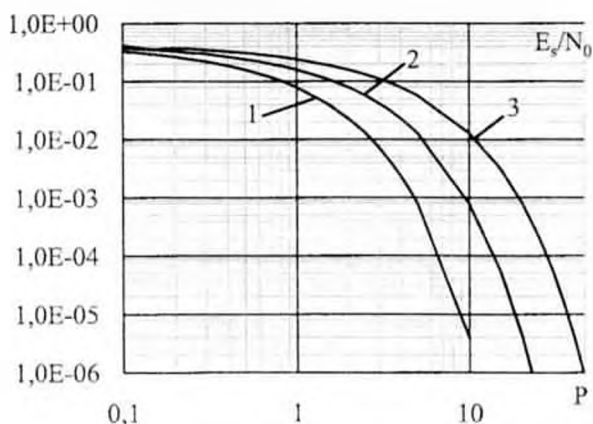


Рис. 1. Зависимость вероятности ошибки от отношения энергии сигнала к спектральной плотности шума  $E_s/N_0$ .

На рис.1. изображены кривые зависимости вероятности ложного приема противофазных, ортогональных сигналов и сигналов с пассивной паузой, рассчитанные по формулам (1.5), (1.6) и (1.7).

На рис.1. представлены сигналы: 1 – противофазные, 2 – ортогональные, 3 – с пассивной паузой.

Пропускная способность  $C$  определяется при максимальной скорости передачи  $R_{\max}$ .

Заимствуем из работы [2] коэффициенты  $\beta$  и  $\gamma$  для определения энергетической и частотной эффективности средств перехвата информации:

$$\beta = C/q; \quad (1.8)$$

$$\gamma = C/W, \quad (1.9)$$

где  $q = P_s/N_0 W$  - отношение мощности сигнала к мощности шума,  $N = N_0 W$ ,

$N_0$  - спектральная плотность мощности шума,

$W$  - полоса частот сигнала.

Коэффициент  $\beta$  характеризует удельную скорость передачи информации относительно  $q$ . Коэффициент  $\gamma$  характеризует скорость передачи информации в единичной полосе частот.

Предельная зависимость  $\beta = f(\gamma)$  при соответствующих способах передачи и прisma определяется по формуле, устанавливающей предел Шеннона (рис.2.) [1, 2]:

$$\beta = \gamma / (2^\gamma - 1). \quad (1.10)$$

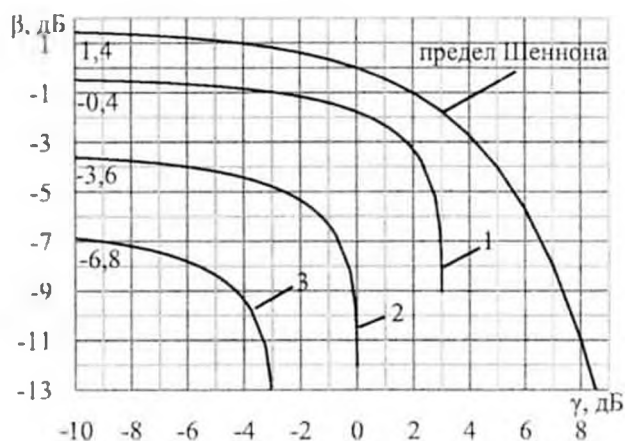


Рис.2. Зависимости предельной эффективности

Построение кривых 1, 2, 3 рис.2. для ДСК при поэлементном приеме осуществляется по выражениям [2]:

$$\gamma = 1/\tau W (1 - Q(P)); \quad (1.11)$$

$$\beta = \gamma / q, \quad (1.12)$$

где  $\tau$  - длительность символа.

На рис.2. представлены сигналы: 1 - противофазные, 2 - ортогональные, 3 - с пассивной паузой.

Предельные кривые представленные на рис.2. для сигналов 1, 2, 3 позволяют устанавливать максимально возможные уровни сигналов в каналах утечки информации.

Установим критерий защищенности цифровых речевых сигналов в зависимости от критерия (нормированного показателя) защиты аналогового речевого сигнала.

При малом отношении сигнал-шум для аналогового сигнала значение пропускной способности будет иметь вид [4]:

$$C = 1,443 \cdot W \cdot \frac{P}{N} = 1,443 \frac{P}{N_0} = 1,443 \Delta, \quad (1.13)$$

где  $P/N_0 = \Delta$  - нормативное значение, определяющая защищенность речевого сигнала по пропускным способностям этих сигналов.

Это указывает, что при малом отношении сигнал-шум пропускная способность канала связи прямо пропорциональна отношению сигнал-шум по мощности.

Для определения критерия защищенности цифровых сигналов устанавливаем его зависимость от критерия защищенности аналоговой речи. Эту зависимость установим по равенству пропускной способности этих сигналов, то есть

$$C_{\text{аналог}} = C_{\text{дискр.}} \quad (1.14)$$

Установив пропускную способность для цифрового сигнала (1.13), (1.14) находим вероятность ошибки по формуле (1.4). Предварительно построив табличную и графическую зависимость между  $C$  и  $P$ .

По формулам (1.5), (1.6), (1.7) построена графическая зависимость между  $E_s/N_0$  и  $P$  (рис.1.).

## ВЫВОД

В работе установлен критерий защищенности цифровых двоичных симметричных сигналов, определена его зависимость от критерия защищенности аналоговой речи. Аналогичные критерии можно установить и для многопозиционных сигналов.

Полученные результаты распространены и на другие виды цифровых сигналов.

## ЛИТЕРАТУРА

- [1] Теория передачи сигналов / А.Г. Зюко, Л.М. Финк, Д.Д. Кловский, М.В. Назаров. // Связь. - 1980. - С. 255-257.
- [2] Помехоустойчивость и эффективность систем передачи информации / А.Г. Зюко и др. // Радио и связь. - 1985. - С. 22-30.
- [3] Информационные основы передачи сообщений / П.И. Ключев. // Советское радио. - 1966. - С. 90-97; 254-256.