УДК 621.372.037.372

МЕТОД ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ, ПРЕОБРАЗОВАННОЙ В ЦИФРОВУЮ ФОРМУ

д-р техн. наук, проф. В.К. ЖЕЛЕЗНЯК, Д.С. РЯБЕНКО
(Полоцкий государственный университет)

Рассматривается передача информации по сетям связи и системам передачи информации, связанная с опасностью её использования несанкционированными пользователями. При создании систем передачи информации особое внимание уделяется обеспечению конфиденциальности. Показаны наиболее уязвимые места возможной утечки информации для цифровых систем передачи информации – прямое и обратное преобразование электрических аналоговых сигналов в цифровую форму, осуществляемое с помощью аналогово-цифровых и цифро-аналоговых преобразователей. Приведены выражения для оценки информационных показателей, определяющих защищенность цифровых и аналоговых сигналов по единому критерию. Данные выражения позволят реализовать автоматизированную измерительную систему для оценки защищенности информации, преобразованной в цифровую форму, в каналах ее утечки.

Передача информации, преобразованной в цифровую форму, обладает несомненными преимуществами перед передачей аналоговой информации. Благодаря достижению высокого предельного качества и уровня достоверности передачи цифровых данных усложнились способы защиты от утечки информации.

При несомненном преимуществе качества цифровой информации, ее защита от утечки по техническим каналам сдерживается отсутствием единого критерия защищенности информации аналоговой и цифровой речевой информации.

Аналоговый первичный речевой сигнал является биологическим. В этой связи его преобразование в цифровую форму предусматривает натуральность восстановленной речи для качественного восприятия. Передача цифровых речевых сигналов по каналам связи (передача данных) обусловлена рядом преобразований из-за того, что цифровые сигналы должны передаваться по аналоговым каналам (каналам тональной частоты), т.е. соответствовать спектральной эффективности.

Критерием оценки защищенности аналоговой речевой информации является нормированное значение величины разборчивости речи [1]. Задача заключается в выборе обоснованного единого критерия для аналоговой и цифровой речи. Сложность этой задачи заключается в многообразии форм представления цифровых сигналов. Из этого многообразия целесообразно рассмотреть их сигнальные конструкции, в первую очередь ортогональные, у которых коэффициент взаимной корреляции равен нулю. К этим сигналам относят частотно-модулированные (ЧМ) сигналы. Другой большой класс – сигналы, у которых коэффициент корреляции не равен нулю. К таким сигналам следует отнести фазомодулированные (ФМ) сигналы.

Передача данных осуществляется передачей элементарных посылок постоянного тока либо посылками элементарного синусоидального сигнала. Важная роль в формировании сигналов передачи данных принадлежит тактовой синхронизации [2].

Целью настоящей работы является обоснование применения двоичных сигналов для оценки защищенности в каналах утечки информации цифровых сигналов с различными их структурными характеристиками и параметрами, указанными выше.

Для этого необходимо проанализировать структурные характеристики и параметры сигналов в каналах утечки информации.

Математическая модель канала передачи информации должна обеспечивать возможность нахождения основных характеристик потока ошибок, что позволит по аналогии оценить защищенность аналоговых и цифровых сигналов в каналах утечки информации. Модель такого канала передачи информации должна быть простой и удобной для проведения расчетов, точно описывать канал передачи информации. Предложена модель двоичного симметричного канала (ДСК).

В работе[3] рассматривают ДСК, распределение ошибок которого определяется следующим образом:

$$P_n(r) = C_n^r P_{ош}^r (1 - P_{ош})^{n-r}, \quad (1)$$

где n – число символов в блоке; r – число ошибочных символов; C_n^r – число сочетаний из n элементов по r; $P_{ош}$ – вероятность ошибки.

Зная вероятность ошибки $P_{ош}$ и используя выражение (1), можно найти все необходимые характеристики.

Отношение сигнал/шум является одним из важнейших параметров системы связи. Этот параметр используют для оценки защищенности канала утечки информации. В цифровых системах передачи информации в качестве критерия качества передачи используется отношение энергии бита сигнала E_b к спектральной плотности мощности шума N_0. Энергия бита E_b оценивается как произведение мощности бита P_b на его длительность T. Время передачи является обратной величиной скорости передачи информации R ($T = 1/R$). Спектральная плотность мощности шума N_0 – величина прямо пропорциональная мощности шума $P_ш$ и обратно пропорциональная ширине полосы сигнала F. В формуле (2) показано математическое представление отношения энергии сигнала к спектральной плотности мощности шума [2]:

$$\frac{E_b}{N_0} = \frac{P_c \cdot T}{P_ш / F} = \frac{P_c / R}{P_ш / F}. \quad (2)$$

Следующим параметром системы передачи информации, преобразованной в цифровую форму, является пропускная способность канала C.

Критерием оценки различных систем передачи информации может служить формула К.Е. Шеннона [4]:

$$C = F \log\left(1 + P_c / P_ш\right). \quad (3)$$

Как следует из формулы (3), пропускная способность гауссовского канала C (бит/с) определяется шириной полосы сигнала F(Гц), отношением мощности сигнала P_c (Вт) к мощности ограниченного полосой F аддитивного белого гауссовского шума $P_ш$ (Вт).

Пропускная способность канала утечки информации должна быть минимальной и определяться пределом Шеннона для сигналов с учетом вероятности ошибки.

Применительно к системе передачи информации пропускная способность гауссовского канала C должна быть максимальна. Этим обеспечивается верность воспроизведения информации, т.е. степень соответствия принятого сообщения переданному сообщению. Верность воспроизведения зависит как от полосы пропускания системы передачи, так и от отношения мощности сигнала к мощности шума. При этом ширина полосы сигнала должна быть меньше ширины полосы канала, а отношение мощности сигнала к мощности шума должно быть максимальным. Так, для речевого сигнала это отношение должно быть не менее 20 дБ. Требования к каналу утечки информации противоположны требованиям к системе передачи информации, т.е. пропускная способность должна быть минимальна.

Из формулы (3) следует, что возможен обмен отношения сигнал/шум на пропускную способность канала. При таких условиях гауссовский канал может работать при значительном превышении мощности шума над мощностью сигнала. При заданной верности воспроизведения возможно обеспечить надежный обмен информацией с учетом требований по ее скрытности.

Зададим пропускную способность C такой, чтобы она соответствовала невозможности извлечения информации из канала утечки информации.

Для симметричного дискретного канала пропускная способность канала C в битах на один отсчет вычисляется [5]:

$$C = \frac{W}{N}\left[\log_2 M + P_{ош} \log_2 \frac{P_{ош}}{M-1} + (1-P_{ош}) \log_2 (1-P_{ош})\right], \quad (4)$$

где $P_{ош}$ – вероятность ложного приема N-мерного сигнала в M-позиционной системе; W – ширина полосы частот. Зависимость C/W от P при различных значениях M представлена на рисунке 1.

Критерий защищенности речевого сигнала в аналоговой форме должен адекватно соответствовать критерию цифрового речевого сигнала.

Установив значение критерия защищенности речевого сигнала в цифровой форме, решим задачу разработки методики оценки защищенности речевого сигнала в цифровой форме.

Из формулы (4) при $M = 2$ получаем пропускную способность C для ДСК [6]:

$$C = 1 + P_{ош} \log_2 P_{ош} + (1-P_{ош}) \log_2 (1-P_{ош}). \quad (5)$$

Шеннон показал [7], что пропускная способность C канала с аддитивным белым гауссовым шумом является функцией средней мощности принятого сигнала P_c, средней мощности шума и ширины полосы пропускания F.

$$C = F \log\left(1 + P_c / P_ш\right). \quad (6)$$

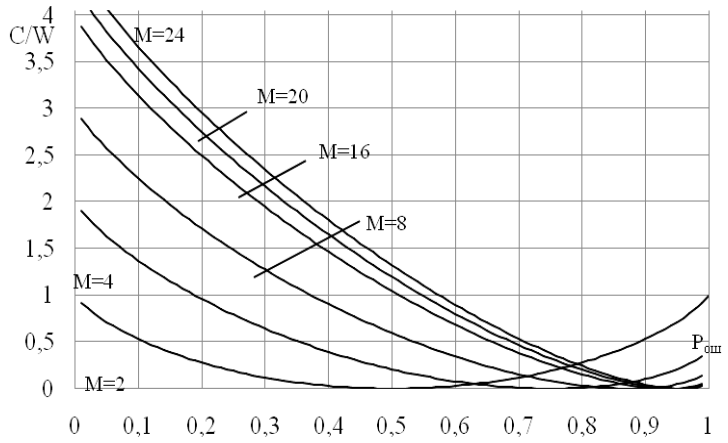

Рис. 1. Зависимость C/W от P при различных значениях M

При малом отношении сигнал/шум для аналогового сигнала из формулы (6) значение пропускной способности принимает вид [7]:

$$C = 1,443 \cdot F \cdot \frac{P}{N} = 1,443 \frac{P}{N_0} = 1,443\Delta, \tag{7}$$

где $P/N_0 = \Delta$ – нормативное значение, по которому установлено определять защищенность аналогового речевого сигнала.

Это указывает, что при малом значении отношения мощности сигнала к спектральной плотности шума пропускная способность системы передачи речевой информации прямо пропорциональна отношению сигнал/шум по мощности.

Предложено [8] критерий защищенности цифровых речевых сигналов установить по известному нормативному критерию защищенности аналоговой его зависимость от критерия защищенности аналоговой речи Δ. Примем для канала с шумами равенство пропускных способностей аналогового и цифрового сигналов, то есть

$$C_{аналог.} = C_{дискр.}. \tag{8}$$

Приняв значение пропускной способности, рассчитанной по формуле (7), для цифрового канала, вычисляют вероятность ложного приема $P_л$.

Получив численное значение $P_л$ по формулам зависимости $P_л = f(E_s/N_0)$ для ортогональных, противоположных сигналов и сигналов с пассивной паузой и графикам, построенным по этим формулам, определяют отношение E_s/N_0.

Нормативным значением следует принять как величину вероятности ложного приема $P_л$, так и отношение энергии бита сигнала к спектральной плотности шума E_s/N_0 для рассмотренных нами сигналов по формулам (9) – (11).

Представлены зависимости $P_л = f(E_s/N_0)$ по видам сигналов [6]:

- сигналы противофазные

$$P_л = Q\left(-\sqrt{2 \cdot E_s/N_0}\right); \tag{9}$$

- сигналы ортогональные

$$P_л = Q\left(-\sqrt{E_s/N_0}\right); \tag{10}$$

- сигналы с пассивной паузой

$$P_л = Q\left(-\sqrt{1/2 \cdot E_s/N_0}\right). \tag{11}$$

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

$$Q(x) = 1/\sqrt{2\pi} \cdot \int_x^{\infty} e^{-\frac{t^2}{2}} dt. \tag{12}$$

По формулам (9) – (11) построена графическая зависимость между E_s/N_0 и $P_л$ (рис. 2).

На практике необходимо решать обратную задачу. Измерив вероятность ложного приема $P_л$ либо отношение энергии бита сигнала к спектральной плотности шума E_s/N_0, определяют величину пропускной способности $C_{дискр.}$. Принято $C_{дискр.} = C_{аналог.}$, по числовому значению $C_{аналог.}$ определяют отношение $\eta = P_c/P_ш$ и сравнивают с нормированной численной величиной Δ.

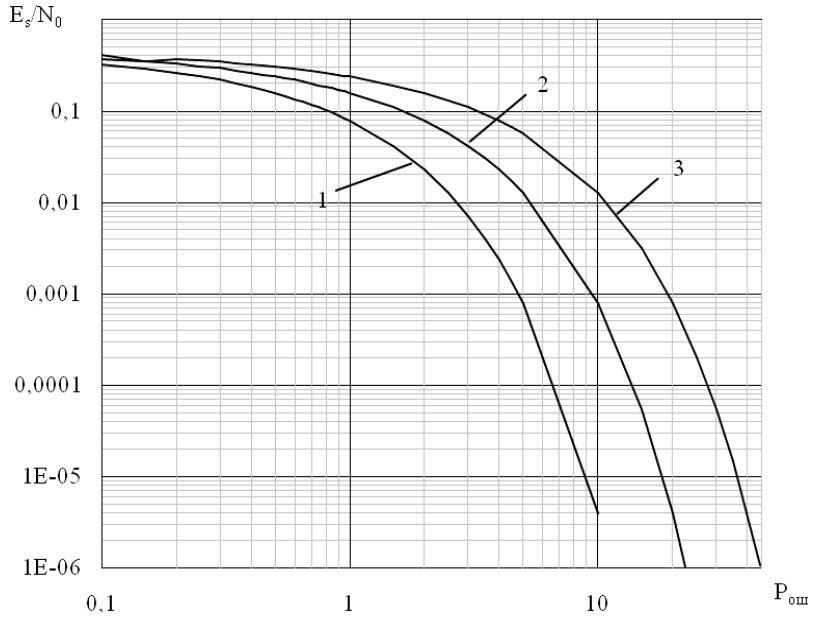

Рис. 2. Зависимость вероятности ошибки $P_{ош}$
от отношения энергии сигнала к спектральной плотности шума E_s/N_0.

Еще одной важной характеристикой цифровой системы передачи информации является его вычислительная скорость R_0, которая используется для определения границы случайного кодирования. Она показывает, что если использовать достаточно длинные коды, то при кодовой скорости R, меньшей вычислительной скорости R_0, среднюю вероятность ошибки можно сделать сколь угодно малой [6].

$$P_{ош} < 2^{-n(R_0-R)}, \tag{13}$$

где $P_{ош}$ – вероятность ошибки; R_0 – вычислительная скорость; R – скорость кодирования.

Минимальное отношение энергии символа к спектральной плотности шума должно соответствовать выражению [6]:

$$\frac{E_s}{N_0} > \frac{1}{2}R(2^{2r}-1). \tag{14}$$

Выражение (14) определяет связь предела Шеннона (минимального отношения сигнал/шум) со скоростью кодирования R.

В работе [9] установлено предельное значение отношения сигнал/шум для необработанного сигнала в зависимости от значения нормированной пропускной способности, называемое пределом Шеннона. Шеннон определил, что при нижнем предельном значении $E/N_0 = 0{,}693 = -1{,}6$ дБ ни при какой скорости передачи нельзя осуществить безошибочную передачу информации. Пропускная способность канала утечки речевой информации должна быть минимальна. Минимальная пропускная способность такого канала обеспечивается условиями, когда ширина полосы сигнала больше ширины полосы канала, а отношение мощности сигнала к мощности шума минимально.

Защищенность в каналах утечки информации цифровых сигналов определяется помехоустойчивостью каналов передачи цифровых сигналов. Потенциальная помехоустойчивость для цифровых систем передачи информации определяется вероятностью ошибки или вероятностью возникновения ошибочного бита.

На основании анализа данных параметров разработан метод оценки защищенности передаваемой информации в канале ее утечки при передаче сигнала по цифровой системе передачи. Также, применяя в качестве критерия формулу Шеннона, можно оценить пропускную способность гауссовского канала, используя сигнал с различными видами манипуляции.

При определении используемого вида манипуляции пытаются достичь максимальной скорости передачи информации, минимальной вероятности ошибки, уменьшения энергетических затрат, минимальной используемой полосы частот. Достичь максимального выполнения данных условий на практике невозможно ввиду их взаимной противоречивости.

Применяются следующие виды манипуляции: амплитудная, частотная, фазовая и их разновидности.

Вероятность ошибки при когерентном приеме в присутствии белого гауссового шума является убывающей функцией отношения энергии сигнала к спектральной плотности шума и возрастающей функцией коэффициента взаимной корреляции [12]

$$P_{ош} = 1 - Q\left(\frac{E_c(1-\rho)}{N_0}\right), \tag{15}$$

Вероятность ошибки ДСК при когерентном приеме для фазовой, частотной и амплитудной манипуляций определяется общим выражением [5]:

$$P_{ош} = 1 - Q\left(\kappa\sqrt{E_c / N_0}\right), \tag{16}$$

где к – коэффициент вида модуляции (к $\sqrt{2}$ = при ФМ, к = 1 при ЧМ, к = $1/\sqrt{2}$ при АМ); E_c/N_0 – отношение энергии сигнала к спектральной плотности мощности шума.

Фазовая модуляция обладает большей помехоустойчивостью, чем амплитудная и частотная. Спектр сигнала ФМ для различных значений Δφ представлен на рисунке 3.

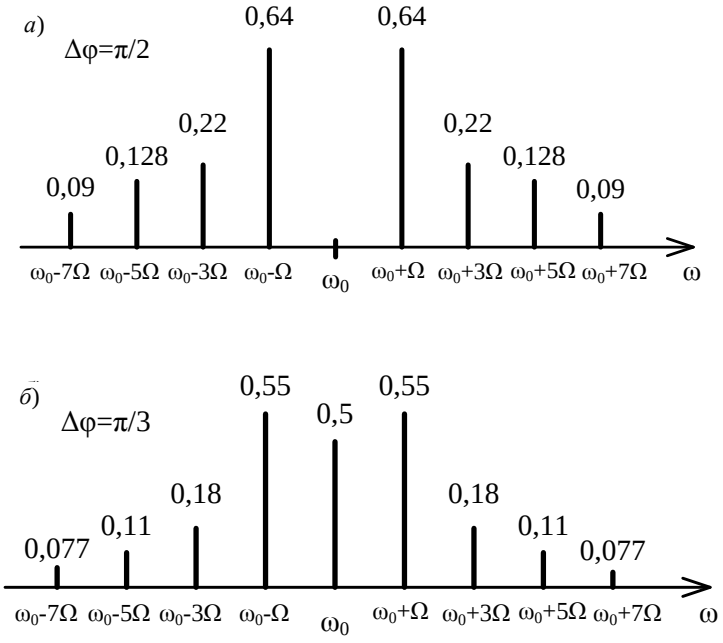

Рис. 3. Спектр сигнала ФМ для различных значений Δφ

Спектр такого сигнала состоит из несущего колебания и нескольких боковых полос. Амплитуда несущего колебания меняется в зависимости от значения Δφ. При увеличении Δφ от 0 до π/2 амплитуда несущего колебания уменьшается до нуля, а амплитуды боковых полос увеличиваются. Когда Δφ = π/2, вся энергия сигнала содержится только в боковых полосах, амплитуда несущего колебания равна 0. При отсутствии несущей составляющей в спектре сигнала (Δφ = π/2) в каналах утечки информации восстановление сигнала будет происходить более затруднительно, чем при наличии несущей.

Сравнение двоичных и *M*-арных систем связи производят с учетом приемника информации [10]. Двоичные системы связи без декодирования и многократные системы связи с двоичным декодированием эквивалентны, так как в обоих случаях на входе получателя информация представлена в виде двоичных символов. В данном случае при сравнении таких систем связи сравнивают вероятности ошибки, приходящиеся на один двоичный символ.

Рассмотрим случай определения вероятности ошибки *M*-арных ортогональных сигналов. При когерентном детектировании вероятность ошибки *M*-арных ортогональных сигналов вычисляется по следующей формуле [9]:

$$P_{ошM} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \left[1 - \left(\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y} e^{-x^2/2} dx \right)^{M-1} \right] \exp\left[-\frac{1}{2} \left(y - \sqrt{\frac{2E_s}{N_0}} \right) \right] dy . \quad (17)$$

Если символьная средняя вероятность ошибки E_b, то для перевода в битовую $E_s = kE_b$, где k – коэффициент, выражаемый из формулы:

$$P_b = \frac{2^{k-1}}{2^k - 1} P_M \approx \frac{P_M}{2}, k >> 1. \quad (18)$$

Рассмотрим зависимость вероятности ошибки от отношения энергии сигнала к спектральной плотности мощности шума (рис. 4).

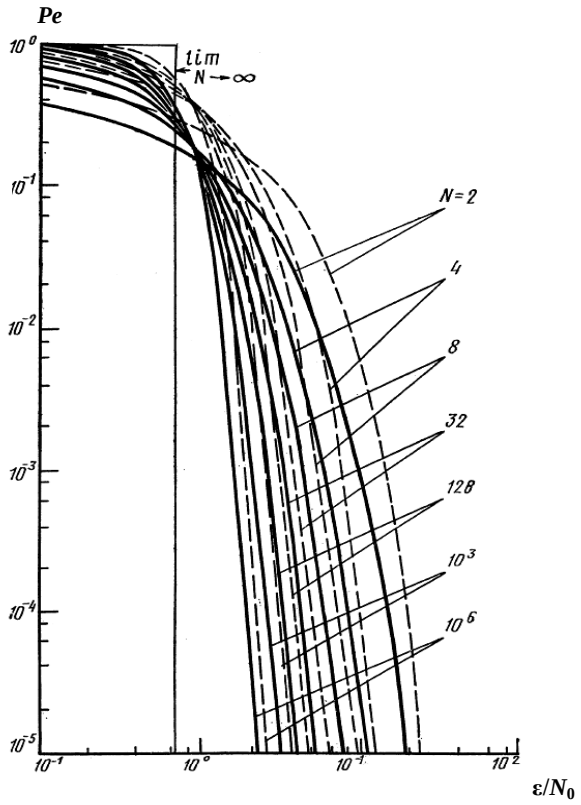

Рис. 4. Зависимость вероятности ошибки от отношения энергии сигнала к спектральной плотности мощности шума [2; 11]

Из графика видно, что с увеличением числа символов *M* уменьшается отношение сигнал/шум на бит, требуемое для заданной вероятности ошибки на бит. При этом получают энергетический выигрыш для ДСК, который определяется как разность между отношениями сигнал/шум при $M = 2$ и $M >> 2$, при условии одинакового значения вероятности ошибки.

Минимальное значение E_b/N_0 для достижения произвольной малой вероятности ошибки при *M*, стремящемся к бесконечности, определяется пределом Шеннона –1,6 дБ для канала с белым гауссовым шумом [2].

Вероятность ошибки в *M*-арном символе сигнала ФМ-М определяется для различных *M* [13].

Так,

- для $M = 2$

$$P_{ош} = Q\left(\sqrt{2\frac{E}{N_0}}\right); \quad (19)$$

для $M = 3$

$$P_{ош} = Q\left(\sqrt{\frac{3E}{2N_0}}\right) + 2T\left(\sqrt{\frac{3E}{2N_0}} \cdot \frac{1}{\sqrt{3}}\right), \tag{20}$$

где $T(x, y)$ – интеграл вероятности, функция Д. Оуэна [13]:

$$T(h,a) = \frac{1}{2\pi}\int_h^{\infty}\int_0^{ax} \exp\left[-\frac{1}{2}\ x^2 + y^2\ \right]dxdy;$$

- для $M = 4$

$$P_{ош} = 2Q\left(\sqrt{\frac{E}{N_0}}\right)\left(1 - \frac{1}{2}Q\left(\sqrt{\frac{E}{N_0}}\right)\right). \tag{21}$$

Критерием оценки цифровых систем передачи данных может служить пропускная способность.

При сравнении двоичных и многопозиционных систем связи установлено [10], что наилучшей помехоустойчивостью обладают многопозиционные системы связи. В каналах утечки информации таких систем с заданным отношением сигнал/шум восстановить исходный передаваемый сигнал гораздо сложнее, чем в двоичных системах связи.

Применение многомерных сигналов позволяет снизить среднюю вероятность ошибки, а увеличение числа символов M приводит к повышению удельной скорости передачи информации [2]. Применение многомерных сигналов позволяет повысить эффективность передачи сообщений.

Широкое применение на практике получили сигналы квадратурной амплитудной модуляции (КАМ). При одинаковом числе сигналов в ансамбле сигналы КАМ обеспечивают более высокую энергетическую эффективность по сравнению с сигналами ФМ, АМ и ЧМ.

Сигналы КАМ обладают большими значениями минимального межточечного расстояния d_{min}, чем АМ и ФМ, а следовательно и большим значением помехоустойчивости [13].

Средняя вероятность ошибки для M-арного символа КАМ-М ($M = 2^k$, k – четно) равна [13]

$$P_{ош} = 4\left(1 - \frac{1}{\sqrt{M}}\right)Q\left(\frac{d}{\sqrt{2N_0}}\right)\left[1 - \left(1 - \frac{1}{\sqrt{M}}\right)Q\left(\frac{d}{\sqrt{2N_0}}\right)\right], \tag{22}$$

где $\frac{d}{\sqrt{2N_0}} = \sqrt{\frac{h_m^2}{(\sqrt{M}-1)^2}} = \sqrt{\frac{3h_c^2}{M-1}};\ \ h_m^2 = \frac{E_m}{N_0};\ \ h_c^2 = \frac{E_c}{N_0}.$

Сравним характеристики качества КАМ и ФМ для заданного объема сигналов M.

Оба типа сигналов являются двухмерными. Аппроксимация вероятности ошибки на символ M-позиционной ФМ выглядит следующим образом [13]:

$$\sqrt[p]{M_{фм}} \approx 2Q\left(\sqrt{2\gamma s} \cdot \sin\frac{\pi}{M}\right).$$

Аппроксимация вероятности ошибки на символ M-позиционной КАМ представлена в виде [13]

$$P_{Mкам} = 2\left(1 - \frac{1}{M}\right)Q\left(\sqrt{\frac{3}{M-1}\frac{E_{ср}}{N_0}}\right).$$

Отношение двух аргументов Q-функции [13]

$$K_M = \frac{P_{Mкам}}{\sqrt[p]{M_{фм}}} = \frac{3(M-1)}{2\sin^2(\pi/M)}.$$

Заключение. Установлены зависимости для сигналов сложной формы КАМ, АФМ, а также зависимости для двоичных и многопозиционных сигналов. Это позволяет оценивать защищенность систем передачи информации по единому нормированному показателю – вероятности ошибки на бит информации. Предложен метод оценки защищенности цифровых систем передачи данных с использованием двоичных симметричных сигналов. Сравнительную оценку можно проводить по графикам (например, рис. 4) [2; 11 – 13].

ЛИТЕРАТУРА

1. Железняк, В.К. Защита информации от утечки по техническим каналам: учеб. пособие / В.К. Железняк; ГУАП. – СПб., 2006. – 188 с.
2. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – 2-е изд.; пер. с англ. – М.: Издат. Дом «Вильямс», 2007. – 1104 с.
3. Дядюнов, А.Н. / Адаптивные системы сбора и передачи аналоговой информации. Основа теории / А.Н. Дядюнов, Ю.А. Онищенко, А.И. Сенин. – М.: Машиностроение, 1988. – 288 с.
4. Защищенные радиосистемы цифровой передачи информации / П.Н. Сердюков [и др.]; под общ. ред. П.Н. Сердюкова. – М.: АСТ, 2006. – 403 с.
5. Помехоустойчивость и эффективность систем передачи информации / А.Г. Зюко [и др.]; под общ. ред. А.Г. Зюко. – М.: Радио и связь, 1985. – 272 с.
6. Золотарев, В.В. Помехоустойчивое кодирование. Методы и алгоритмы: справ. / В.В. Золотарев, Г.В. Овечкин; под ред. Ю.Б. Зубарева. – М.: Горячая линия – Телеком, 2004. – 126 с.
7. Клюев, Л.Л. Теория электрической связи / Л.Л. Клюев. – Минск: Дизайн ПРО, 1998. – 336 с.
8. Способ оценки защищенности от утечки речевого сигнала: пат. 15588 Респ. Беларусь МПК J L 15/00, H04R 29/00 / В.К. Железняк, Д.С. Рябенко: заявитель Полоц. гос. ун-т. – № a 20100293; заявл. 01.03.2010; опубл. 30.04.2012 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2012. – № 2(85). – С 165 – 166.
9. Прокис, Д. Цифровая связь; пер. с англ. / Д. Прокис; под ред. Д.Д. Кловского. – М.: Радио и связь, 2000. – 800 с.
10. Варакин, Л.Е. Системы связи с шумоподобными сигналами / Л.Е. Варакин. – М.: Радио и связь, 1984. – 384 с.
11. Стиффлер, Дж.Дж. Теория синхронной связи / Дж.Дж. Стиффлер; пер. с англ. Б.С. Цыбакова; под ред. Г.М. Габидулина – М.: Связь, 1975. – 488 с.
12. Витерби, Э.Д. Принципы когерентной связи / Э.Д. Витерби; пер. с англ.; под ред. Б.Р. Левина. – М.: Сов. радио, 1966. – 392 с.
13. Савищенко, Н.В. Многомерные сигнальные конструкции: их частотная эффективность и потенциальная помехоустойчивость приема / Н.В. Савищенко; под ред. Д.Л. Бураченко. – СПб.: Изд-во Политехн. ун-та, 2005. – 420 с.

Поступила 10.09.2012

METHOD OF ESTIMATION OF SECURITY OF INFORMATION TRANSFORMED INTO THE DIGITAL FORM

V. ZHELEZNYAK, D. RYABENKO

The information transfer through communication networks and information transfer systems is connected with the danger of use of this information by not authorized users. Considerable efforts are spent on maintenance of confidentiality of the transferred information when creating systems of information transfer. Direct and return transformations of electric analogue signals into the digital form are the weakest spots of possible information leakage for digital systems of information transfer, carried out by means of analogue-to-digital and digital-to-analogue converters. In the given work expressions for estimation of the information indicators defining security of digital and analogue signals by uniform criterion are presented. The given expressions will allow to realize the automated measuring system for estimation of security of the information transformed into the digital form, in channels of its leak.