УДК 621.372.037.372

ОБОСНОВАНИЕ ОПТИМАЛЬНОГО СИГНАЛА ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ ЦИФРОВЫХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

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

Исследуется оптимальный сигнал для оценки защищенности цифровых каналов утечки информации. Технология технической защиты информации формирует обобщенные требования к теории и технике передачи систем сигналов. Рассматривается система сигналов, используемая для передачи информации как совокупность сигналов, объединяемых единым правилом построения. Известно, что помехоустойчивость – одно из основных требований к системе передачи. Предложены оптимальная система сигналов, обеспечивающая максимальную помехоустойчивость при минимальных отношениях энергии бита к спектральной плотности мощности шума в каналах утечки информации, методы оценки защищенности дискретных систем сигналов в каналах утечки информации при воздействии шумов высокого уровня типа белого гауссовского шума, а также выбор и обоснование оптимального сигнала, который позволит оценить защищенность цифровых каналов утечки информации.

Защищенность цифровых сигналов в канале утечки информации основана на формировании исходных требований, учитывающих свойства канала передачи сигнала, характеристики и параметры формируемых сигналов для передачи и их структуру. Сигнал канала передачи оценивают средней мощностью передачи сигнала, его искажением, которое определяется отношением энергии бита к спектральной плотности мощности шума. Обеспечение помехоустойчивости при приеме сигналов является важной задачей. Помехоустойчивость при воздействии шумов обеспечивают когерентным либо некогерентным приемом сигналов, их видами.

Основная часть. Виды сигналов различают по их цифровой модуляции. Нами будут рассмотрены фазоманипулированные сигналы (ФМн), частотно-манипулированные (ЧМн), амплитудно-манипулированные (АМн) и сигналы с квадратурно-амплитудной модуляцией (КАМ).

Системы сигналов обладают пороговым эффектом. В качестве критерия оценки влияния канала передачи на канал утечки информации может служить пропускная способность, которая определяется по формуле К.Е. Шеннона [1]:

$$C = W_c \log_2(1 + S/N). \quad (1)$$

Как следует из формулы (1), пропускная способность гауссовского канала C (бит/с) определяется шириной полосы сигнала W_c (Гц), отношением мощности сигнала S (Вт) к средней мощности шума N (Вт), ограниченного полосой W_c.

Зависимость энергии бита (E_b) к спектральной плотности мощности шума (N_0) от нормированной полосы пропускания канала представлена на рисунке 1 [1, с. 550].

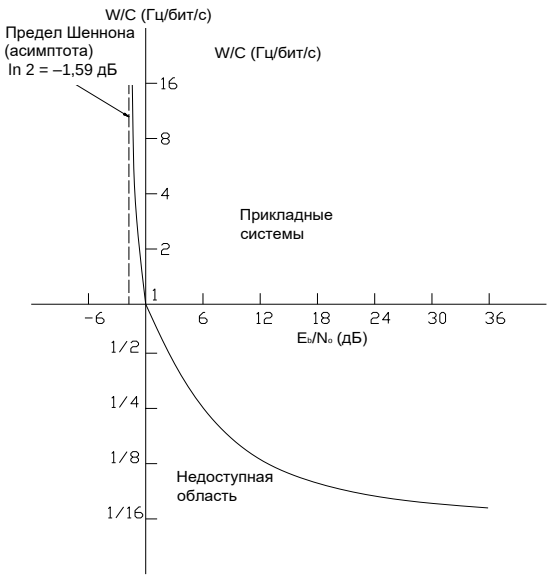


Рис. 1. Зависимость E_b/N_0 от нормированной полосы пропускания канала

При нижнем предельном значении E_b/N_0 = –1,6 дБ, определяющем пороговое значение, ни при какой скорости передачи нельзя осуществить безошибочную передачу информации.

Важным критерием являются методы оценки защищенности дискретных систем сигналов в каналах утечки информации при воздействии шумов высокого уровня типа белого гауссовского шума. Помехоустойчивость зависит от расстояния между сигналами $S_i(t)$ и $S_j(t)$, образующими систему [2]:

$$d(S_i, S_j) = \left\{ \int_0^{T_c} \left[S_i(t) - S_j(t) \right]^2 dt \right\}^{1/2}, \quad (2)$$

где T_c – длительность сигнала.

Помехоустойчивость системы сигналов увеличивается при увеличении расстояния d. Для достижения большего расстояния коэффициент взаимной корреляции должен быть минимальным:

$$d(S_i, S_j) = \left[2E(1 - R_{ij}) \right]^{1/2}. \quad (3)$$

Здесь $R_{ij} = \frac{1}{E} \int_0^{T_c} S_i(t) \cdot S_j(t) dt$ – коэффициент взаимной корреляции между сигналами $S_i(t)$ и $S_j(t)$, принимающий значения в пределах от –1 до +1; E – энергии сигналов $S_1(t) \cdot S_2(t)$.

Согласно [3], для оптимальной системы сигналов $R = -\frac{1}{m-1}$. Это достигается равенством всех коэффициентов корреляции, т.е. $R_{ij} = R$ для всех i и j.

Под оптимальной следует понимать систему сигналов, обеспечивающую максимальную помехоустойчивость при заданных априорных условиях передачи информации.

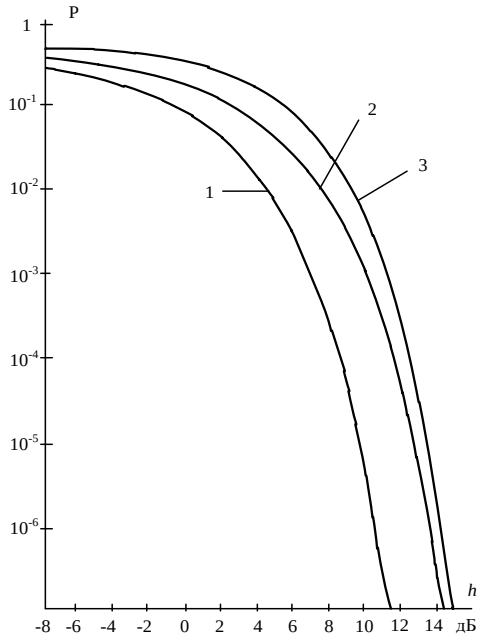


Рис. 2. Зависимость вероятности ошибки P от отношения энергии бита к спектральной плотности мощности шума h

Для детального анализа сигналов необходимо учесть, что отношение сигнал/шум в канале утечки информации гораздо меньше единицы, а их наводки являются несимметричными.

На рисунке 2 представлена зависимость вероятности ошибки P от отношения мощности сигнала к мощности шума h для когерентного *1* приема двоичных ФМн-сигналов, когерентного *2* и некогерентного *3* приема двоичных ЧМн-сигналов [4; 5].

Из рисунка следует, что при малом значении отношения сигнал/шум разброс вероятности ошибок незначителен.

Вероятность ошибки $P_{ош}$ от отношения энергии бита спектральной плотности мощности к мощности шума h для некогерентного приема ЧМ-сигнала представлена зависимостью [1, с. 245]:

$$P_{ош} = \frac{1}{2} \exp\left(-\frac{1}{2} \frac{E_b}{N_0} \right). \quad (4)$$

Зависимость вероятности двоичного ФМ-сигнала от отношения энергии сигнала к спектральной плотности мощности помехи для когерентного приема [3; 6]

$$P_e = 1 - F\left[\sqrt{\frac{2E_b}{N_0}} \right]. \quad (5)$$

Зависимость вероятности ортогональных ЧМн-сигналов на промежутке времени [0, T] при условии равенства энергии сигналов [3]

$$P_e = 1 - F\left[\sqrt{\frac{E_b}{N_0}} \right]. \quad (6)$$

Формирование ортогональных ЧМн- и противоположных ФМн-сигналов основано на определенных закономерностях.

Заданы два гармонических колебания [3]:

$$\left.\begin{aligned} S_k(t) &= A_k \cos(w_k t + \varphi_k), \\ S_m(t) &= A_m \cos(w_m t + \varphi_m). \end{aligned}\right\} \quad (7)$$

Определяют условия, при которых эти колебания являются ортогональными сигналами в промежутке времени [0, T] [3]:

$$\int_0^T S_k(t) \cdot S_m(t) = 0 . \quad (8)$$

Для ЧМн-сигналов условие ортогональности соблюдается при равенстве нулю взаимной энергии двух гармонических колебаний $S_k(t)$ и $S_m(t)$ в промежутке времени [0, T] [3]:

$$E(S_k, S_m) = \int_0^T A_k A_m \cos(w_k t + \varphi_k)\cos(w_m t + \varphi_m)dt = 0 . \quad (9)$$

Равенство нулю (9) достигается дополнительными условиями.

Условие 1 – начальные фазы $\varphi_k = \varphi_m = 0$ на промежутке времени [0, T], ортогональность сигналов достигается подбором частот [3]:

$$\left.\begin{aligned} (w_k t + \varphi_k)T &= \chi_1 \pi, \\ (w_m t + \varphi_m)T &= \chi_2 \pi, \end{aligned}\right\} \quad (10)$$

где $(\chi_1, \chi_2) = 1, 2, 3\ldots$

Из (10) определяют частоты, удовлетворяющие условиям ортогональности:

$$\left.\begin{aligned} w_k &= \frac{(\chi_1 + \chi_2)\pi}{2T}, \\ w_m &= \frac{(\chi_1 - \chi_2)\pi}{2T}. \end{aligned}\right\} \quad (11)$$

Условие 2 – начальные фазы $\varphi_k = \varphi_m$, ортогональность сигналов достигается подбором фаз [3]:

$$\sin\left[(w_k + w_m)T + \varphi_k + \varphi_m\right] - \sin(\varphi_k + \varphi_m) = 0 , \quad (12)$$

при $\omega_k = \omega_m$.

При одинаковых частотах, определяемых из условия $\omega_k = \chi_1\pi/T$, сигналы являются ортогональными, если сдвиг фаз между ними равен $\pm\pi/2$.

Условие 3 – сигналы $S_k(t)$ и $S_m(t)$ противофазны: $\varphi_k = -\varphi_m$ [3].

Двоичные системы передают одну двоичную единицу (или один бит) информации. Алфавит, содержащий n символов, передает $\log_2 n$ двоичной единицы информации на каждый символ. Посредством многопозиционной манипуляции несущего колебания по амплитуде, частоте и фазе формируют m-ичные сигналы, используя $m = 2^k$, где k – количество двоичных единиц в символе. Применение сигналов с многопозиционной АМн возможно в каналах с низким уровнем аддитивного шума.

Различия между системами передачи информации определяются объемом алфавита источника n и сигнала m. В зависимости от m системы передачи информации разделяют на двоичные ($m = 2$) и m-ичные ($m > 2$).

На рисунке 3 [4; 5] показана зависимость вероятности ошибочного приема символа от нормированного отношения сигнал/шум, определяемого как отношение сигнал/шум, приходящееся на двоичную единицу информации [4]:

$$h_2 = \frac{h_k}{k} = h_m \log_2 m . \quad (13)$$

Кривые построены для сигналов с многопозиционной фазовой манипуляцией при $m = 2, 4, 8, 16$ и 32.

Из рисунка 3 следует, что при малом отношении сигнал/шум h_2 (дБ) < 0 для $m = 2$ вероятность ошибочного приема символа меньше, чем для $m > 2$. В этой связи сигнал с двухпозиционной ФМн имеет

предпочтение перед сигналами с $m > 2$, так как, не обнаружив двоичный ФМн сигнал в шумах при отношении сигнал/шум < 0 (дБ), можно гарантировать защищенность сигналов многопозиционного сигнала.

При некогерентном приеме начальная фаза неизвестна и является случайной величиной [2]. Наибольшая помехоустойчивость имеет место при передаче двоичной информации ортогональными сигналами.

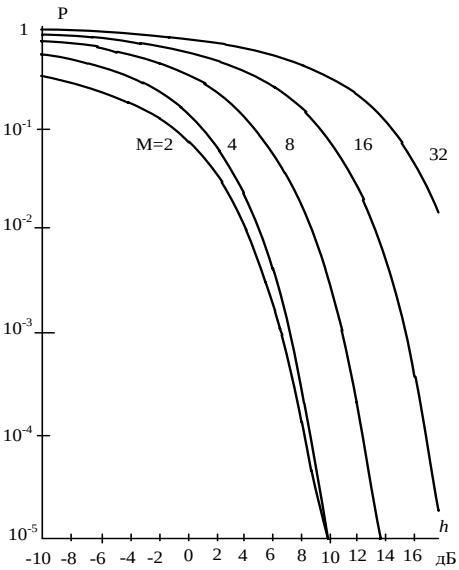


Рис. 3. Зависимость вероятности ошибки P от отношения мощности сигнала к мощности шума h для когерентного ФМн сигнала

Вероятность ошибки при некогерентном приеме двух ортогональных сигналов определяется из формулы (4). Помехоустойчивость когерентного и некогерентного приема двух ортогональных сигналов отличается незначительно.

Широкое применение на практике получили сигналы КАМ. При одинаковом числе сигналов в ансамбле сигналы КАМ обеспечивают более высокую энергетическую эффективность по сравнению с сигналами ФМн, АМн, ЧМн. Сигналы КАМ обладают большими значениями минимального межточечного расстояния $d_{\min}$, чем АМн и ФМн, а следовательно, и большим значением помехоустойчивости [6].

Средняя вероятность ошибки для КАМ-М при $m = 2^k$ (k – четно) на m-арный символ равна [6]

$$P_{ош} = 4\left(1-\frac{1}{\sqrt{m}}\right)Q\cdot\left(\frac{d}{\sqrt{2N_0}}\right)\left[1-\left(1-\frac{1}{\sqrt{m}}\right)Q\cdot\left(\frac{d}{\sqrt{2N_0}}\right)\right], \quad (14)$$

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

Сравним характеристики качества КАМ и ФМн для заданного объема сигналов m. Оба типа сигналов являются двухмерными.

Аппроксимация вероятности ошибки на символ m-позиционной ФМн выглядит следующим образом [6]:

$$P_{\sqrt{m_{\text{ФМн}}}} \approx 2Q\left(\sqrt{2\gamma_s}\sin\frac{\pi}{m}\right). \quad (15)$$

Аппроксимация вероятности ошибки на символ m-позиционной КАМ представлена в виде [6]

$$P_{m_{KAM}} = 2\left(1-\frac{1}{\sqrt{m}}\right)Q\left(\sqrt{\frac{3}{m-1}\frac{E_{cp}}{N_0}}\right). \quad (16)$$

Отношение двух аргументов Q-функции [6]

$$K_m = \frac{P_{m_{KAM}}}{P\sqrt{m_{\text{ФМн}}}} = \frac{3/(m-1)}{2\sin^2(\pi/m)}. \quad (17)$$

Из ряда работ следует, что наилучшей помехоустойчивостью обладает двоичная система сигналов с фазовой манипуляцией ФМн при когерентном приеме, отношение сигнал/шум которой [7]

$$h = \sqrt{\frac{2E}{N_0}}, \quad (18)$$

где N_0 – спектральная плотность мощности шума.

При $m > 2$ преимущества ФМн снижаются из-за взаимного влияния, обусловленного взаимной корреляцией между сигналами.

В многопозиционной системе ЧМн символы передаются с различными значениями частоты. Некогерентный прием ортогональных сигналов ЧМн (рис. 4) в области нормированного отношения сиг-

нал/шум на двоичную единицу h_2 (дБ) меньше 0 дБ имеют ту же зависимость от вероятности ошибочного приема P, т.е. двоичная система ($m = 2$) имеет преимущество по сравнению с системами $m > 2$.

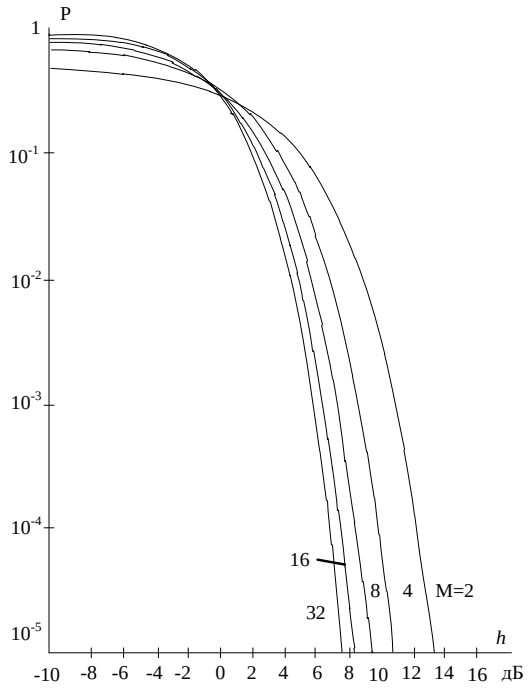


Рис. 4. Зависимость вероятности ошибки P от отношения мощности сигнала к мощности шума h для некогерентного ЧМн сигнала [4]

Отношение сигнал/шум для m-арного символа связано с отношением сигнал/шум на двоичную единицу [4]

$$h_2 = \frac{h}{k}. \qquad (19)$$

Вероятность ошибки [4]

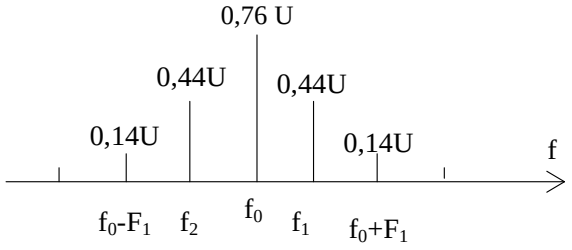
$$P_l < m \cdot \exp\left(-k\frac{h_2}{2}\right) = \exp\left[-k\left(\frac{h_2}{2} - \ln 2\right)\right].$$

Вероятность ошибочного приема экспоненциально стремится к нулю при условии, что отношение сигнал/шум на двоичную единицу удовлетворяет неравенству [4]

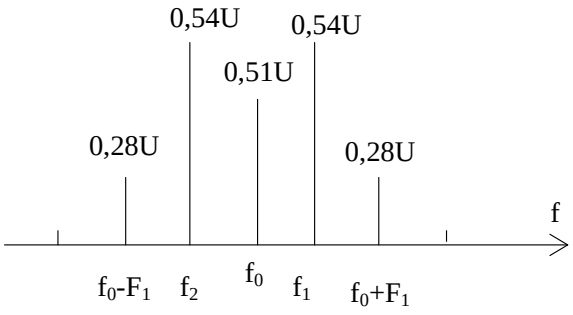
$$h_2 > \ln 2. \qquad (20)$$

При пороговых значениях, если энергия сигнала на двоичный символ превышает спектральную плотность мощности шума в 1,39 раза, можно говорить об использовании двоичного ортогонального сигнала в качестве измерительного в канале утечки информации, учитывая его преимущества в большей чувствительности и несинхронности системы.

Формирование двоичного ортогонального сигнала рассмотрено в литературе [8]. Спектр ЧМн сигнала представлен на рисунке 5.



а)



б)

Рис. 5. Спектр ЧМн сигнала:
а – для $k_{ЧМн} = 0{,}8$; *б* – для $k_{ЧМн} = 1{,}2$ [8]

Из рисунка 5 следует, что при малых значениях коэффициента модуляции $k_{ЧМн}$ энергия колебания сосредоточена в полосе частот вблизи несущей частоты f_0. При этом ширина спектра колебания ЧМн сиг-

нала без разрыва фазы равна ширине спектра колебания АМн. По мере увеличения коэффициента $k_{чМн}$ энергия ЧМн сигнала концентрируется в области боковых частот.

Заключение. В результате проведенной работы предложено для оценки защищенности цифровых каналов утечки информации использовать в качестве измерительных двоичные ортогональные некогерентные сигналы без разрыва фазы, зависимости вероятности ошибки от отношения мощности сигнала к мощности шума которых находятся вблизи границы Шеннона.

ЛИТЕРАТУРА

1. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – 2-е изд. пер. с англ. – М.: Издат. дом «Вильямс», 2007. – 1104 с.
2. 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.
3. Клюев, Н.И. Информационные основы передачи сообщений / Н.И. Клюев. – М.: «Связь», 1966. – 360 с.
4. Стейн, С. Принципы современной теории связи и их применение к передаче дискретных сообщений / С. Стейн, Дж. Джонс; отв. ред. Л.М. Финк. – М.: «Связь», 1971. – 376 с.
5. Витерби, Э.Д. Принципы когерентной связи / Э.Д. Витерби; пер. с англ. под ред. Б.Р. Левина. – М.: «Советское радио», 1966. – 392 с.
6. 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.
7. Варакин, Л.Е. Теория систем сигналов / Л.Е. Варакин. – М.: «Сов. радио», 1978. – 304 с.
8. Железняк, В.К. Основы теории модулированных колебаний: учебное пособие / В.К. Железняк, С.В. Дворников. – СПб.: ГУАП, 2006. – 160 с.

Поступила 19.04.2013

STUDY OF AN OPTIMAL SIGNAL FOR THE ESTIMATION OF SAFETY OF DIGITAL CHANNELS OF INFORMATION LEAKAGE

V. ZHELEZNYAK, D. RYABENKO

An optimal signal for the estimation of safety of digital channels of information leakage is studied. The technology of technical protection of information forms generic requirements to the theory and technique of transmission of systems of signals. The system of signals is considered, which is used for transmission of information as a total of signals, united by an integrated rule of construction. It is known, that noise immunity is one of the main requirements to the system of transmission. An optimal system of signals, providing maximal noise immunity at minimal ratio of bit energy to the spectral density of noise power in the channels of information leakage, methods of estimation of safety of discrete signal systems in the channels of information leakage under the influence of high level noises like Gaussian white noise and the choice and explanation of an optimal signal, which will allow to estimate the safety of digital channels of information leakage are proposed.