УДК 621.372.037.372

МЕТОД СИГНАЛА ОРТОГОНАЛЬНОЙ ЧАСТОТНОЙ МАНИПУЛЯЦИИ БЕЗ РАЗРЫВА ФАЗЫ ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ ОТ УТЕЧКИ РЕЧЕВЫХ СИГНАЛОВ В ЦИФРОВОЙ ФОРМЕ

В.К. ЖЕЛЕЗНЯК, Д.С. РЯБЕНКО

Полоцкий государственный университет
Блохина, 29, Новополоцк, 211440, Беларусь

Поступила в редакцию 11 октября 2013

Исследуется оптимальный частотно-манипулированный сигнал для оценки защищенности каналов утечки информации в цифровой форме. Рассматривается система сигналов, используемая для передачи информации как совокупность сигналов, объединяемых единым правилом построения. 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 каналов утечки информации.

Ключевые слова: речевой сигнал, манипуляция сигнала, спектр сигнала, оценка защищенности сигнала.

Введение

Защита информации от утечки определяется многими факторами. Мера защиты дискретных сообщений определяется методом, реализующим предельную чувствительность, высокую точность, помехозащищенность. Помехозащищенность измерительного сигнала для оценки защищенности каналов утечки информации является одним из основных факторов, влияющим на предельную чувствительность и высокую точность. Первичное преобразование аналоговых сигналов в цифровые (дискретные) последовательности, которыми манипулируют несущие частоты, генерирует каналы утечки информации.

Цель работы – предложить и обосновать структуру и основные параметры оптимального измерительного сигнала и оценку защищенности от утечки (дискретных) манипулированных сигналов в цифровой форме.

Основной задачей является обработка сигнала в условиях шумов высокого уровня. В этой связи возникает необходимость сужения полосы такого сигнала, оптимальность его обработки. Выбор измерительного сигнала решается при воздействиях ряда факторов, неопределенность которых не исследована. Принципы системного подхода для обоснования основных параметров измерительного сигнала характеризуют степень достижения поставленной цели оценки защиты информации.

Выбор измерительного сигнала

Для передачи дискретных сообщений широко распространены двоичные ($M = 2$) и М-ичные ($M > 2$) амплитудно-манипулированные (АМн), частотно-манипулированные (ЧМн) и фазоманипулированные (ФМн) сигналы. Манипулированный сигнал представляет собой несущие колебания, параметры которого меняются во времени по частоте или по фазе.

Модулирующими сигналами являются биты, важные параметры которых – коэффициент взаимной корреляции ρ, энергия символьного бита. Символьные биты сформированы видеоимпульсами. Векторная структура определяется величиной коэффициента взаимной корреляции некоторого множества битового символа ($M = 2$ либо $M > 2$). ФМн-сигналы, модулирующие несущее колебание $f_н$ при $\rho = -1$, минимизируют вероятность ошибочного приема бита. Для М-ичных ФМн-сигналов вероятность символьной ошибки P_E увеличивается из-за взаимной корреляции между битами, уменьшения отношения энергии бита $E_б$ к спектральной плотности мощности шума N_0, т.е. $E_б/N_0$. С увеличением размера множества символов $M = 2^k$, где $k = 2, 4, 8, 16\ldots$, энергия символа $E_E = E_б \cdot \log_2 M$.

В табл. 1. [2] представлены вероятности ошибки для различных бинарных манипуляций при $M = 2$. Из [2] следует, что разность между когерентной ФМн и некогерентной ЧМн составляет приблизительно 4 дБ при вероятности ошибки бита 10^{-4}. При когерентном детектировании бинарных ФМн сигналов и некогерентном детектировании бинарных ортогональных ЧМн-сигналов [2] вероятность ошибки составляет $8 \cdot 10^{-1}$ и $5 \cdot 10^{-1}$ бит соответственно при $E_б/N_0$ минус 8 дБ. Увеличение $M = 2^k$ повышает вероятность битовой ошибки ФМн-передачи и уменьшает вероятность ошибки при ортогональной ЧМн-передаче. Разность вероятностей битовой ошибки ЧМн ($M = 2$) для когерентного и некогерентного приема составляет менее 1 дБ при отношении $E_б/N_0 = -10$ дБ [3].

На основании исследований модулирующих сигналов можно сделать вывод о необходимости дальнейшего исследования ортогонального ЧМн-сигнала с некогерентным приемом.

При малых отношениях $E_б/N_0 = -10$ дБ выигрыш в чувствительности когерентного сигнала по отношению к некогерентному составляет менее одного дБ. М-ичная передача ЧМн-сигналов по чувствительности имеет несомненное преимущество перед ФМн-сигналами.

При некогерентном приеме начальная фаза неизвестна, являясь случайной величиной. Вероятность ошибки при оптимальном некогерентном приеме двух ортогональных сигналов [4]:

$$P_с = 0{,}5\exp\left(-0{,}5h_0^2\right) = 0{,}5\exp\left(-0{,}5\,E_б \big/ N_0\right), \text{ где } h_0^2 = \frac{P_с T}{N_0} = \frac{E_б}{N_0}.$$

Анализ АМн-сигналов, обладающих более низкой помехоустойчивостью по сравнению с ФМн- и ЧМн-сигналами, исследовать нецелесообразно. Численные значения коэффициентов зависимости между ФМн-, ЧМн- и АМн-сигналами известны [5, 6].

Решение задачи начнем с анализа известных методов передачи информации, преобразованной в цифровую форму. При различном числе символов (алфавит включает $\log_2 M$ бит информации), остановимся на двоичных ЧМн-сигналах, имеющих преимущество перед ФМн и АМн при системном анализе. Из многообразия и сложности структуры и функций измерительных сигналов рассмотрим ортогональный сигнал частотной манипуляции [2]:

$$S_i = \sqrt{\frac{2E}{T}}\cos(\omega_i t + \varphi),\ 0 \le t \le T,\ i = \overline{1, M}.$$

Сигналы $S_i(t)$ и $S_j(t)$, имеющие одинаковую длительность и действующие на интервале от $t_1 = t_0$ до $t_2 = t_0 + T$, называются ортогональными, если их скалярное произведение равно нулю [1]:

$$\int_0^{t_0+T} S_i(t) \cdot S_j(t)\,\mathrm{d}t = 0,$$

а спектры этих сигналов удовлетворяют условию

$$\int_{-\infty}^{\infty} S_i(jt) \cdot S_j^*(jt)\,\mathrm{d}t = 0.$$

Сигналы $S_i(t)$ и $S_j(t)$ с несущими частотами f_1 и f_2 являются ЧМн-несущими $i, j = \overline{1, M}, i \ne j$.

Обоснование ЧМн-сигнала в качестве измерительного для оценки защищенности от утечки речевых сигналов в цифровой форме

Передача речевых сигналов в цифровой форме по каналам связи и сигналов передачи данных обусловлена рядом преобразований. Передача данных осуществляется манипуляцией несущих элементарными битовыми символьными посылками.

Некогерентная ортогональная передача ЧМн-сигналов, характеризующаяся отсутствием перекрестных искажений при передаче несущих гармонических колебаний частот f_1 и f_2 длительностью T с одинаковыми амплитудами, подтверждает их ортогональность. Частоты f_1 и f_2 ортогональны, если разность частот (f_1–f_2) кратна 1/T Гц [2]. Такая разность устанавливается при воздействии тактовых частот, благодаря чему отсутствуют перекрестные помехи. Минимальная разность между несущими частотами f_1 и f_2 для двоичных ортогональных ЧМн-сигналов $\cos(2\pi f_1 t+\varphi)$ и $\cos 2\pi f_2 t$. Такие сигналы формируются при $f_1 > f_2$, скорости $1/T$ символ/с, где T – длительность символа, φ – произвольный постоянный уровень фазы между 0 и 2π.

Ортогональность удовлетворяется, если [2]:

$$\int_0^T \cos 2\pi f_1 t \cdot \cos 2\pi f_2 t \, \mathrm{d}t - \sin\varphi \int_0^T \sin 2\pi f_1 t \cdot \cos 2\pi f_2 t \, \mathrm{d}t = 0.$$

После ряда преобразований

$$\cos\varphi \cdot \sin 2\pi(f_1 - f_2)T + \sin\varphi\left(\cos 2\pi(f_1 - f_2)T - 1\right) = 0.$$

Выражение справедливо при произвольной фазе φ, если $\sin 2\pi(f_1–f_2)=0$ и $\cos 2\pi(f_1–f_2) = 1$ $\sin x = 0$, $\cos x = 1$ при $n = 2k$.

Из [2] $2\pi(f_1 – f_2)T = 2\pi k$ или $f_1 – f_2 = 1/T$. Минимальная разность частот между несущими f_1 и f_2 для ортогональной передачи ЧМн сигнала с некогерентным детектированием достигается при $k = 1$ [2].

Ортогональность несущих частот f_1 и f_2 достижима с исключением перекрестных искажений при тактовой синхронизации, если при передаче сигнала с несущей f_1 не принимается сигнал на несущей f_2 фильтром приемника, настроенным на несущую f_2.

Проанализируем спектры ЧМн-колебаний с целью сравнительной оценки их параметров для использования в качестве измерительного сигнала. Синтез такого сигнала возможен для оценки защищенности от утечки в несимметричных зашумленных каналах утечки информации.

Аналитическое выражение спектра двоичных ЧМн-колебаний представляется как сумма двух независимых модулированных сигналов [7]:

$$U_{\text{ЧМн}}(t) = U'_{f1}(t) + U''_{f2}(t),$$

где $U'_{f1}(t)$ – спектр сигнала с несущей f_1, $U''_{f2}(t)$ – спектр сигнала с несущей f_2.

Спектр сигнала с несущей f_1 [7]:

$$U'_{f1}(t) = U_m \frac{t_u}{T}\cos\omega t + U_m \frac{t_u}{T}\sum_{k=1}^{\infty} \frac{\sin\dfrac{kF_1 t_u}{2}}{\dfrac{kF_1 t_u}{2}} \cdot \left[\cos(\omega + kf_1)t + \cos(\omega - kf_1)t\right]. \qquad (1)$$

Из (1) следует, что спектр АМн-колебания имеет две симметричные боковые полосы с частотами ($\omega \pm kf_1$), $k = 1, 2, \ldots, n$.

Представим модулирующее колебание в виде меандра [8]:

$$E(t) = \frac{4E}{\pi}\left(\sin\omega_0 t + \frac{1}{3}\sin 3\omega_0 t + \frac{1}{5}\sin 5\omega_0 t + \ldots\right) = \frac{4E}{\pi}\sum_{n=0}^{\infty}\frac{\sin(2n+1)\omega_0 t}{(2n+1)\omega_0 t},$$ где $\omega_0 = 2\pi/T$, $n = 1, 2 \ldots i$.

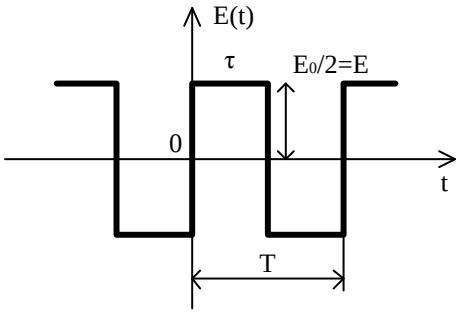

Рис. 1. Модулирующее колебание в виде меандра (T – период, τ – длительность импульса).

Представим АМн-колебание [7]:

$$U''_{f2}(t)=U_m\left(1-\frac{t_u}{T}\right)\cos 2\pi f_2 t-U_m\frac{t_u}{T}\sum_{k=1}^{\infty}\frac{\sin\dfrac{2\pi kF_1t_u}{2}}{\dfrac{2\pi kF_1t_u}{2}}\cdot\left[\cos(2\pi f_2+2\pi kF_1)t+\cos(2\pi f_2-2\pi kF_1)t\right].$$

Окончательное выражение спектра ЧМн-сигнала с разрывом фазы представляется выражением:

$$U_{\text{ЧМн}}(t)=U_m\frac{t_u}{T}\cos 2\pi f_2 t+U_m\left(1-\frac{t_u}{T}\right)\cos 2\pi f_2 t+U_m\frac{t_u}{T}\sum_{k=1}^{\infty}\frac{\sin\dfrac{2\pi kF_1t_u}{2}}{\dfrac{2\pi kF_1t_u}{2}}\times$$

$$\times\left[\cos(2\pi f_1+2\pi kF_1)t+\cos(2\pi f_1-2\pi kF_1)t-\cos(2\pi f_2+2\pi kF_1)t-\cos(2\pi f_2-2\pi kF_1)t\right].$$

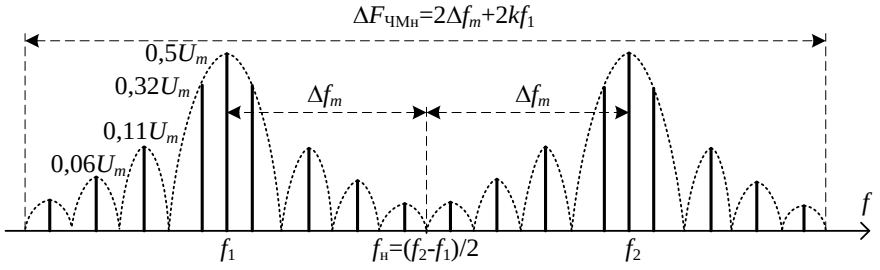

Рис. 2. Спектр двоичного ЧМн-сигнала.

Из представленного на рис. 2 графика следует, что спектр ЧМн-сигнала занимает полосу $\Delta F_{\text{ЧМн}}=2\Delta f_m+2kF_1$. Ширина спектра определяется числом k учитываемых гармоник F_1, разностью частот (f_2-f_1), значением частоты f_1 и первой верхней модулирующей частотой меандра.

Из рис. 2 следует, что спектр колебаний ЧМн шире спектра АМн при прочих равных условиях на величину удвоенной девиации частоты $2\Delta f_m$. Сравнительную оценку параметров ЧМн-сигнала с разрывом фазы и без разрыва фазы выполним с представления выражения спектра колебаний ЧМн-сигнала без разрыва фазы.

Спектр ЧМн-сигнала без разрыва фазы представляется выражением [7]:

$$U_{\text{ЧМн}}(t)=U_m\cos\left[2\pi f_{\text{н}}t+\Delta\varphi(t)\right], \qquad (2)$$

где $\Delta\varphi(t)$ – приращение фазы, обусловленная изменением частоты $f_{\text{н}}$. Представим (2) в развернутом виде:

$$U_{\text{ЧМн}}(t)=U_m\left[\cos 2\pi f_{\text{н}}t\cdot\cos\Delta\varphi(t)-\sin 2\pi f_{\text{н}}t\cdot\cos\Delta\varphi(t)\right].$$

Для построения спектра ЧМн-сигнала необходимо развернуть функции $\cos\Delta\varphi(t)$ и $\sin\Delta\varphi(t)$. Модулирующим сигналов по-прежнему является меандр. С помощью этого сигнала происходит изменение частоты $f_{\text{н}}$ на величину $\pm\Delta f_m$ [9]:

$$\Delta f(t)=\begin{cases}-\Delta f_m \ \text{ при } -t_{\text{и}}<t<0;\\ \Delta f_m \ \text{ при } 0<t<t_{\text{и}}.\end{cases}$$

Изменение $\Delta f(t)$ фазы $\Delta\varphi(t)$ зависит от изменения частоты [9]:

$$\Delta\varphi(t)=\int_0^t \Delta f(t)dt=\begin{cases}-\Delta f_m t+C_1, -t_u<t<0;\\ \Delta f_m t+C_2, 0<t<t_u,\end{cases} \qquad (3)$$

где C_1 и C_2 – постоянные интегрирования, которые целесообразно выбрать таким образом, чтобы соблюдались условия непрерывности фазы, определяемые из рис. 3 [7].

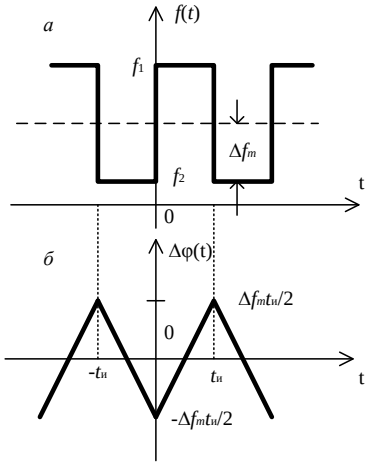

Рис. 3. Манипулирующее колебание (меандр) (*а*), приращение фазы в ЧМн-колебании (*б*)

Тогда из (3), используя значения C_1 и C_2 получаем

$$\Delta\varphi(t)=\begin{cases}-\Delta f_m t\left(t+t_{\text{и}}/2\right), -t_{\text{и}}<t<0;\\ \Delta f_m t\left(t-t_{\text{и}}/2\right), 0<t<t_{\text{и}}.\end{cases}$$

Функции $\cos\Delta\varphi(t)$ и $\sin\Delta\varphi(t)$ периодические, поскольку функция $\Delta\varphi(t)$ периодическая. Функции $\cos\Delta\varphi(t)$ и $\sin\Delta\varphi(t)$ были разложены в ряд Фурье и получено [7]:

$$U_{\text{ЧМн}}(t)=\frac{a_0}{2}=U_m\frac{\sin\frac{\pi m_{\text{чм}}}{2}}{\frac{\pi m_{\text{чм}}}{2}}\cos 2\pi f_{\text{н}}t+\frac{2m_{\text{чм}}U_m}{\pi}\sum_{k=2,4,6\ldots}^{\infty}\frac{\frac{\pi m_{\text{чм}}}{2}}{m_{\text{чм}}^2-k^2}\times$$

$$\times\left[\cos\left(2\pi\left(f_{\text{н}}+kF_1\right)t\right)+\cos\left(2\pi\left(f_{\text{н}}-kF_1\right)t\right)\right]-$$

$$-\frac{2m_{\text{чм}}U_m}{\pi}\sum_{k=1,3,5\ldots}^{\infty}\frac{\frac{\pi m_{\text{чм}}}{2}}{m_{\text{чм}}^2-k^2}\times\left[\sin\left(2\pi\left(f_{\text{н}}+kF_1\right)t\right)+\sin\left(2\pi\left(f_{\text{н}}-kF_1\right)t\right)\right].$$

Представим спектр ЧМн колебаний без разрыва фазы при индексе частотной манипуляции m = 0,8.

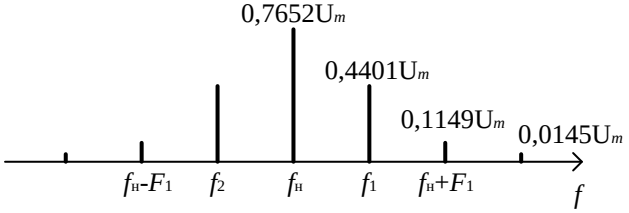

Рис. 4. Спектр ЧМн-колебания при индексе ЧМн $m_{\text{чм}}$=0,8 [7]

Практически можно считать, что спектр ЧМн сигнала имеет две боковые несущие, поскольку остальные несущие составляют порядка двух процентов энергии сигнала. Ширина спектра ЧМн без разрыва фазы равна ширине полосы АМн сигнала.

Заключение

Выбрана и обоснована предпочтительная и актуальная альтернатива применительно к сложной решаемой задаче оценки защищенности речевых сигналов в цифровой форме в виде ортогонального ЧМн-сигнала без разрыва фазы. Метод сигнала с ортогональной частотной модуляцией без разрыва фазы для оценки защищенности от утечки цифровой речевых сигналов в цифровой форме обладает наиболее узкой полосой спектра по сравнению с ФМн, АМн. Метод сигнала с ортогональной частотной модуляцией без разрыва фазы для оценки защищенности от утечки речевых сигналов в цифровой форме занимает полосу спектра в 2 раза уже по сравнению с методами ЧМн сигнала с разрывом фазы, исключая переходные искажения и повышая точность оценки за счет учета с высокой точностью только двух боковых составляющих. Коэффициент k определяется отношением спектра ЧМн-сигнала с разрывом фазы к отношению спектра ЧМн-сигнала без разрыва фазы и составляет при равных несущих частотах $f_н$ и девиации частоты $k = 2$.

METHOD OF ORTHOGONAL FREQUENCY MANIPULATION SIGNAL WITHOUT RUPTURE OF THE PHASE FOR THE ESTIMATION OF SECURITY FROM LEAK OF SPEECH SIGNALS IN THE DIGITAL FORM

V.K. ZHELEZNYAK, D.S. RYABENKO

Abstract

The optimum frequency-manipulated signal for an estimation of security of channels of information leakage in the digital form is investigated. The system of signals used for an information transfer as set of signals, united by a uniform rule of construction is considered. The optimum system of signals providing the maximum noise stability at the minimum relations of energy of bit to spectral density of capacity of noise in channels of information leakage, methods of an estimation of security of discrete systems of signals in information leakage channels are offered at influence of noise of high level of type white noise, and also a choice and a substantiation of an optimum signal which will allow to estimate security of channels of information leakage.

Список литературы

1. *Мановцев А.П.* Введение в цифровую радиотелеметрию. М., 1967.
2. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. М., 2007.
3. *Стиффлер Дж.Дж.* Теория синхронной связи. М., 1975.
4. Защищенные радиосистемы цифровой передачи информации / Под ред. П.Н. Сердюкова. М., 2006.
5. *Савищенко Н.В.* Многомерные сигнальные конструкции: их частотная эффективность и потенциальная помехоустойчивость приема. СПб, 2005.
6. *Рябенко Д.С., Железняк В.К.* // Вестн. ПГУ. Серия С. Фундаментальные науки. 2012. № 12. С. 12–19.
7. *Железняк В.К., С.В. Дворников* Основы теории модулированных колебаний. СПб, 2006.
8. *Гарновский Н.Н.* Теоретические основы электропроводной связи. Часть 1. Общая теория пассивных линейных цепей с сосредоточенными постоянными. М., 1956.
9. *Анго Андре.* Математика для электро- и радиоинженеров. М., 1964.