ОЦЕНКА ЗАЩИЩЕННОСТИ ЦИФРОВЫХ СИГНАЛОВ АМ, ЧМ, ФМ, КАМ В КАНАЛАХ УТЕЧКИ ИНФОРМАЦИИ

УДК 621.397.7:004.056.57

Д.С. Рябенко, В.К. Железняк
ПГУ, г. Полоцк

Аннотация

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

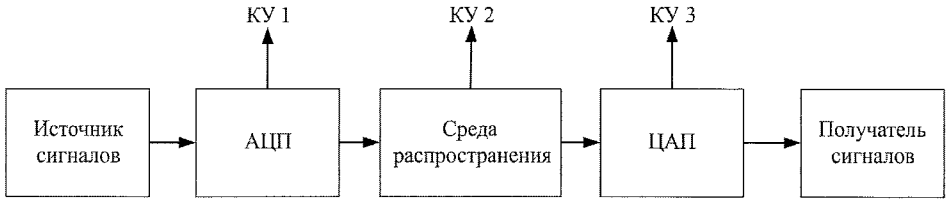

Рисунок 1 – Схема цифровой системы передачи информации с возможными ее каналами утечки информации.

сигнала, который позволит оценить защищенность цифровых каналов утечки информации.

Введение

Защищенность цифровых сигналов в канале утечки информации основана на формировании исходных требований, учитывающих свойства канала передачи сигнала, характеристики и параметры формируемых сигналов для передачи каналом передачи и их структура. Сигнал канала передачи оценивают средней мощностью передачи сигнала, его искажением, оцениваемым отношением энергии бита к спектральной плотности мощности шума, определяющим вероятность ошибки. Важнейшей задачей является обеспечение при их приеме помехоустойчивости, достаточной для малой вероятности ошибки. Помехоустойчивость при воздействии шумов обеспечивают когерентным либо некогерентным приемом сигналов, их видами. Виды сигналов различают по их цифровой модуляции. Нами рассматриваются фазоманипулированные сигналы ФМн, частотно-манипулированные ЧМн, амплитудно-манипулированные АМн и сигналы с квадратурно-амплитудной модуляцией КАМ.

Важным являются методы оценки защищенности дискретных систем сигналов в каналах утечки информации при воздействии шумов высокого уровня типа белого гауссовского шума.

Основная часть

При выявлении технических каналов утечки цифровой системы передачи информации необходимо рассматривать систему, включающую основное (стационарное) оборудование, оконечные устройства, среду распространения, распределительные и коммутационные устройства, системы электропитания, системы заземления.

Схема цифровой системы передачи информации с возможными ее каналами утечки информации представлена на рисунке 1.

На рисунке 1 представлены возможные каналы утечки информации, организуемые полями рассеивания цифрового сигнала: КУ1 – на выходе АЦП, КУ2 – при передаче цифрового сигнала, представленного последовательностью импульсов, по среде распространения, КУ3 – в ЦАП при формировании из цифровой последовательности исходного аналогового сигнала.

В зависимости от природы возникновения информационных сигналов, а также среды их распространения и способов перехвата, технические каналы утечки информации можно разделить на электромагнитные и электрические каналы утечки информации [1].

Токи и напряжения информационных электрических цепей являются источниками магнитных и электрических полей, ослаблены, как правило, неоднородной средой распространения (в том числе, неоднородными экранами). Магнитные и электрические поля наводят токи (напряжения) на неинформационные электрические цепи. Наведенные токи и напряжения распространяются в неинформационных электрических цепях и создают вторичные магнитные и электрические поля, которые могут распространяться на значительные расстояния.

К электромагнитным относятся каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений системы передачи информации – электромагнитные излучения элементов системы передачи информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в электрических и магнитных цепях системы, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания:

– излучений элементов системы передачи информации;

– излучений на частотах работы высокочастотных генераторов;

– излучений на частотах самовозбуждения усилителей низкой частоты.

Для цифровых систем передачи информации характерно наличие побочных электромагнитных излучений элементов системы передачи информации. При аналогово-цифровом преобразовании сигнала, несущего информационную составляющую, его передаче через среду распространения и обратном цифро-аналоговом преобразовании, данный электрический сигнал, при прохождении через элементы системы передачи информации возбуждает электрические и магнитные поля в окружающем пространстве. Эти поля модулированы по закону изменения информационного сигнала. Перехват таких полей может быть осуществлен даже на значительном расстоянии.

Критерием оценки цифровых систем передачи информации может служить помехоустойчивость.

Помехоустойчивость зависит от расстояния между сигналами $d(S_i, S_j)$, образующих систему [2]. Под оптимальной системой следует понимать систему сигналов, обеспечивающую максимальную помехоустойчивость при заданных априорных условиях передачи информации.

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

где T_c – длительность сигнала.

Помехоустойчивость системы сигналов увеличивается при увеличении расстояния d.

Для достижения большего расстояния коэффициент взаимной корреляции должен быть минимальным:

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

где $R_{ij} = \frac{1}{E}\int_0^{T_c} S_i(t)S_j(t)dt$ – коэффициент взаимной корреляции между сигналами $S_i(t)$ и $S_j(t)$, принимающие значения в пределах от -1 до +1, E – одинаковые энергии сигналов.

Для оптимальной системы сигналов $R = -1/(M-1)$[3]. Это достигается равенством всех коэффициентов корреляции, т.е. $R_{ij} = R$ для всех i и j.

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, некогерентного (3) и когерентного (2) приема двоичных ЧМн сигналов [4].

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

Зависимость вероятности двоичного ФМ-сигнала от отношения энергии сигнала E_s к спектральной плотности мощности помехи N_0 для когерентного приема [3]

$$P_e = 1 - F\left[\sqrt{\frac{2E_s}{N_0}}\right]. \quad (3)$$

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

$$P_e = 1 - F\left[\sqrt{\frac{E_s}{N_0}}\right]. \quad (4)$$

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 $m > 2$.

Сравнение двоичных и m-арных систем связи производят с учетом приемника информации [1]. 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 вероятности ошибки m-арных ортогональных сигналов вычисляется по формуле [5]

$$P_{ошM} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\left[1-\left(\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{y} e^{-x^2/2}dx\right)^{M-1}\right]\exp\left[-\frac{1}{2}\left(y-\sqrt{\frac{2E_s}{N_0}}\right)\right]dy \quad (5)$$

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

$$P_b = \frac{2^{k-1}}{2^k - 1}P_M \approx \frac{P_M}{2}, k >> 1 \quad (6)$$

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

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]

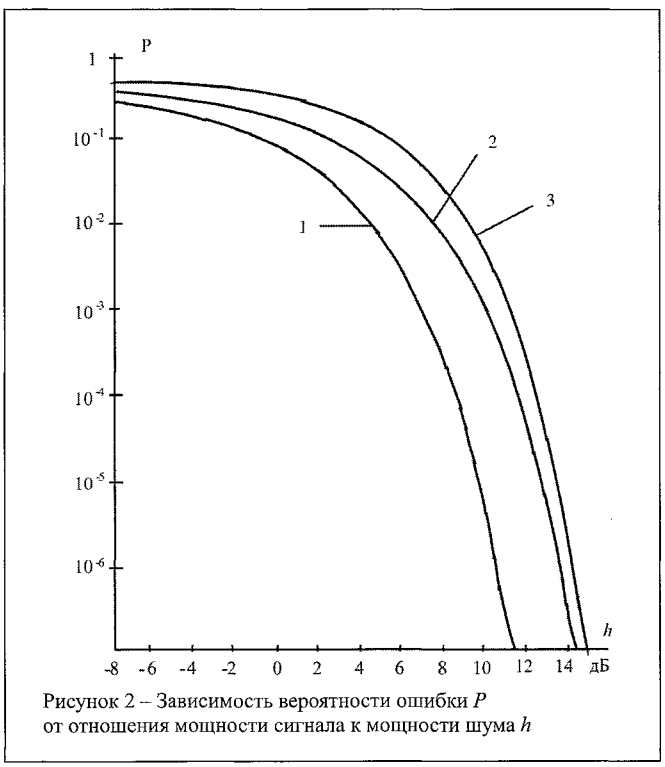

Рисунок 2 – Зависимость вероятности ошибки P от отношения мощности сигнала к мощности шума h

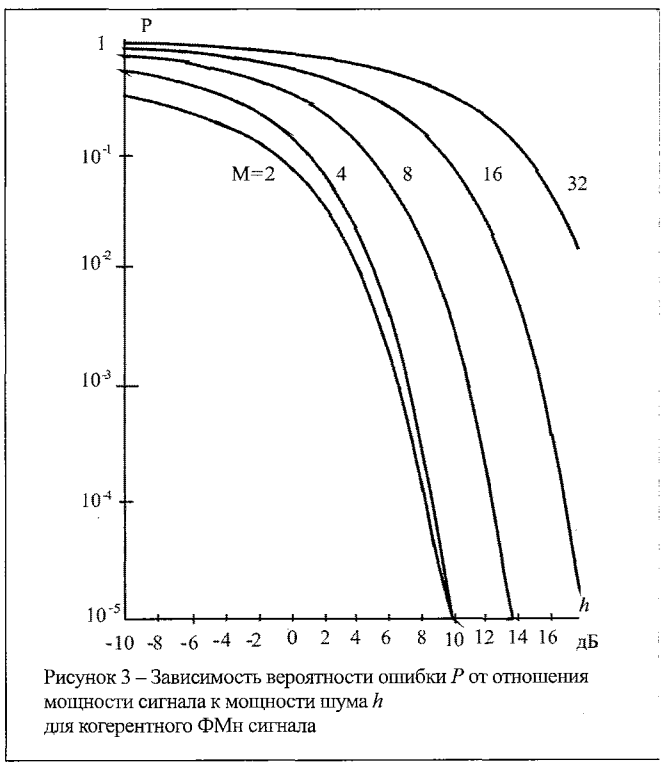

Рисунок 3 – Зависимость вероятности ошибки P от отношения мощности сигнала к мощности шума h для когерентного ФМн сигнала

$$E(S_k,S_m)=\int_0^T A_k A_m \cos(w_k t+\varphi_k)\cos(w_m t+\varphi_m)dt=0\ . \quad (7)$$

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

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

$$h_2=\frac{h_k}{k}=h_m\log_2 M. \quad (8)$$

Из рисунка 3 следует, что при малом отношение сигнал/шум h_2(дБ) < 0 для М = 2 вероятность ошибочного приема символа меньше, чем для М > 2.В этой связи сигнал с двухпозиционной ФМн имеет предпочтение перед сигналами с М > 2, так как не обнаружив сигнал двоичной ФМн сигнала в шумах при отношение сигнал/шум<0 (дБ), можно гарантировать защищенность сигналов многопозиционного сигнала.

При некогерентном приеме начальная фаза неизвестна и является случайной величиной [2]. Наибольшая помехоустойчивость соответствует при передаче двоичной информации ортогональными сигналами. Вероятность ошибки при некогерентном приеме двух ортогональных сигналов выражается [2, 6]:

$$P_{ош}=0{,}5\exp(-0{,}5h_2^2), \quad (9)$$

Помехоустойчивость когерентного и некогерентного приема двух ортогональных сигналов отличается незначительно.

Из ряда работ следует, что наилучшей помехоустойчивостью обладает двоичная система сигналов с фазовой манипуляцией ФМн при когерентном приеме, отношение сигнал/шум которой [6]

$$h=\sqrt{2E_s/N_0}, \quad (10)$$

где N_0 – спектральная плотность мощности шума, E_s – энергия сигнала.

При М > 2 ФМн снижается помехоустойчивость из-за взаимного влияния между сигналами, обусловленного взаимной корреляцией.

В многопозиционной системе ЧМн символы передаются с различными значениями частоты. Некогерентный прием ортогональных сигналов ЧМн (рисунок 4) в области нормированного отношения сигнал/шум на двоичную единицу h_2 (дБ) меньше 0 дБ имеют ту же зависимость от вероятности ошибочного приема Р, т.е. двоичная система (m = 2) имеет преимущество по сравнению с системами m > 2.

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

$$h_2=\frac{h}{k}. \quad (11)$$

Вероятность ошибки [4]

$$P_l\langle Me^{-k\frac{h_2}{2}}=\exp\left[-k\left(\frac{h_2}{2}-\ln 2\right)\right]$$

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

$$h_2\rangle \ln 2.$$

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.

Сигналы КАМ обладают большими значениями минимального межточечного расстояния d, чем АМ и ФМ, а следовательно и большим значением помехоустойчивости [7].

Средняя вероятность ошибки для КАМ-М, $M=2^k$, k – четно, на m-арный символ равна [7]

$$P_{ош}=4\left(1-\frac{1}{\sqrt{M}}\right)Q\left(\frac{d}{\sqrt{2N_0}}\right)\left[1-\left(1-\frac{1}{\sqrt{M}}\right)Q\left(\frac{d}{\sqrt{2N_0}}\right)\right], \quad (12)$$

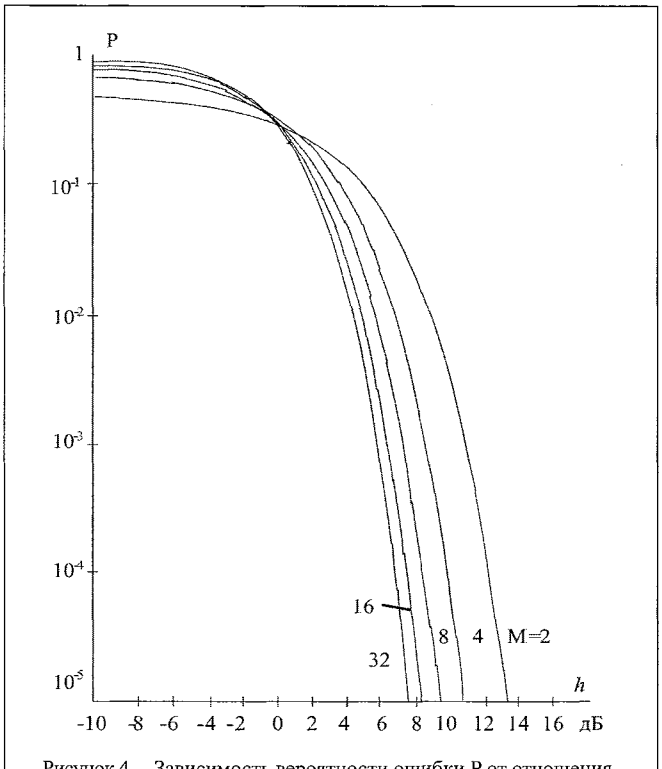

Рисунок 4 – Зависимость вероятности ошибки Р от отношения мощности сигнала к мощности шума h для некогерентного ЧМн сигнала [4].

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 М. Оба типа сигналов являются двухмерными.

Аппроксимация вероятности ошибки на символ М-позиционной ФМ выглядит следующим образом [7]

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

Аппроксимация вероятности ошибки на символ М-позиционной КАМ представлена в виде [7]

$$P_{m\text{КАМ}} = 2\left(1-\frac{1}{\sqrt{m}}\right)Q\left(\sqrt{\frac{3}{m-1}\frac{E_{cp}}{N_0}}\right)$$

Отношение двух аргументов Q-функции [7]

$$K_m = P_{m\text{КАМ}} / P_{\sqrt{m}\text{ФМн}} = \frac{3/(M-1)}{2\sin^2(\pi/M)}$$

Заключение

В ходе работы предложено для оценки защищенности цифровых каналов утечки информации использовать в качестве измерительных двоичные ортогональные когерентные и некогерентные сигналы, зависимости вероятности ошибки от отношения мощности сигнала к мощности шума которых находятся вблизи границы Шеннона. 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.

Литература:

1. Железняк, В.К. Защита информации от утечки по техническим каналам: учебное пособие / В.К. Железняк; ГУАП. – СПб., 2006. – 188 с.

2. Зюко, А.Г. Помехоустойчивость и эффективность систем связи / А.Г. Зюко. – М.: Связьиздат, 1963. – 320 с.

3. Клюев, Н.И. Информационные основы передачи сообщений / Н.И. Клюев. – М.: Московская типография № 10 Главполиграфпрома, 1966. – 360 с.

4. Стейн, С. Принципы современной теории связи и их применение к передаче дискретных сообщений / С. Стейн, Дж. Джонс, отв. редактор Л.М. Финк. – М.: «Связь», 1971. – 376 с.

5. 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.

6. Варакин, Л.Е. Теория систем сигналов / Л.Е. Варакин. – М.: «Сов.радио», 1978. – 304 с.

7. 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.

Abstract

The optimum signal for an estimation of security of digital channels of information leakage is investigated. The technology of technical protection of the information forms the generalized requirements to the theory and techniques of transfer of systems of signals. The system of signals used for an information transfer as set of signals, united by a uniform rule of construction is considered. It is known, that a noise stability – one of the basic requirements to transfer system. 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 Gaussian noise, and also a choice and a substantiation of an optimum signal which will allow to estimate security of digital channels of information leakage.

Поступила в редакцию 18.05.2013 г.

СПОСОБ ПОДАВЛЕНИЯ ЗАШУМЛЕННЫХ ИМПУЛЬСНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПУТЕМ КОМПЕНСАЦИИ

УДК 621.397.7:004.056.57

В.К. Железняк, А.В. Барков,
ПГУ, г. Полоцк

Аннотация

Рассматривается обнаружение периодических импульсных последовательностей и их подавление путем компенсации в канале утечки информации. Задачей является обнаружение периодической импульсной последовательности из аддитивных шумов высокого уровня с целью последующего её подавления. Обнаружение основано на быстром преобразовании Фурье и накоплении сигнала в частотной области. Сравнение и оценку обнаружения производят при помощи оптимального приема и порогового детектирования. Выбор порога осуществляют по известным критериям оптимальности в задачах обнаружения сигналов. Подавление импульсных последовательностей в канале утечки информации решается их компенсацией воспроизведением противофазного обнаруженного сигнала. Эксперименты проведены моделированием периодической импульсной последовательности с добавлением аддитивных шумов, таких как белый шум, хаотическая импульсная последовательность, телеграфный сигнал. Предложен способ обнаружения и компенсация зашумленных импульсных последовательностей. Проанализированы известные