REFERENCES

1. Об образовании в Российской Федерации: федеральный закон // Федеральный портал «Российское образование» [Электронный ресурс]. – 2012. – Режим доступа: http://www.edu.ru.
2. Федеральный государственный общеобразовательный стандарт // Портал «Федеральный государственный общеобразовательный стандарт» [Электронный ресурс]. – 2012. – Режим доступа: http://standart.edu.ru.
3. Daniel, John. New technology in the International Baccalaureate. Technology is the answer. And what is the question? / John Daniel. – 2006.

UDC 621.372.037.372

CHOICE OF THE OPTIMUM SIGNAL FOR THE ESTIMATION OF SECURITY OF DIGITAL CHANNELS OF INFORMATION LEAKAGE

D. RABENKA, V. ZHELEZNYAK
Polotsk State University, Belarus

Maintenance of security of confidential information in technical channels from leakage is one of the directions of technical protection of the information. The choice of binary orthogonal coherent and incoherent signals in information leakage channels is shown in the following article.

Security of signals in digital channels of information leakage is based on initial requirements which include properties of the channel of a signal transmission, characteristics and parameters of formed signals and their structure. Signal of the channel of transfer is estimated by average capacity of a signal transmission and its distortion which is estimated by the relation of energy of bit to spectral density of noise power. Noise power defines an error probability. Signals are divided into two big classes: binary ($m = 2$) and multidimensional ($m > 2$). The major problem is maintenance of noise immunity at their reception which is sufficient for small error probability. Noise immunity is provided by coherent or incoherent reception of signals influenced by noise. Kinds of signals depend on their digital modulation. We consider phase-shift keyed signal, frequency-shift keyed signal, amplitude-shift keyed signal, signals with quadrature- amplitude modulation and signals with pulse-code modulation.

The technology of technical protection of the information forms the generalized requirements for the theory and techniques of transfer of systems of signals. System of signals $\{S_i(t)\}$, $i = 1, 2, \ldots, m$ is used for an information transfer. It is a set of the signals united by a uniform rule of construction. The optimum system of signals provides the maximum noise immunity under the set aprioristic conditions of the information transfer [1], [2].

Methods of valuation of discreet signal system security are important in channels of information leakage when the level of noise is high (for example Gaussian white noise).

The noise immunity depends on distance between the signals, which form [2]:

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

where T_c – duration of a signal.

The noise immunity of system of signals increases when distance d increases.

The coefficient of cross correlation should be minimum in order to increase distance d.

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

where $R_{ij} = \frac{1}{E} \int_0^{T_c} S_i(t) S_j(t) dt$ – the coefficient of cross correlation between signals $S_i(t)$ and $S_j(t)$, which varies from -1 to +1, E – identical energy of signals.

For optimum system of signals $R = -1/M - 1$ [2]. It is reached by equality of all factors of correlation, i.e. $R_{ij} = R$ for all i and j.

It is necessary to understand that the optimum system is the system of the signals that provide the maximum noise stability under a set of priori conditions of information transfer.

For the detailed analysis of signals it is necessary to consider. That the relation a signal/noise in the channel of information leakage is much less than one and their interference are asymmetrical.

Dependence of error probability P on the relation of signal power to noise power h for incoherent (2) and coherent (1) receptions of binary PM signals, incoherent (4) and coherent (3) receptions of binary FM signals are presented in fig. 1 [1], [4].

As seen from the figure, the spread of probability of errors is rather insignificant for small value of the signal/noise relation.

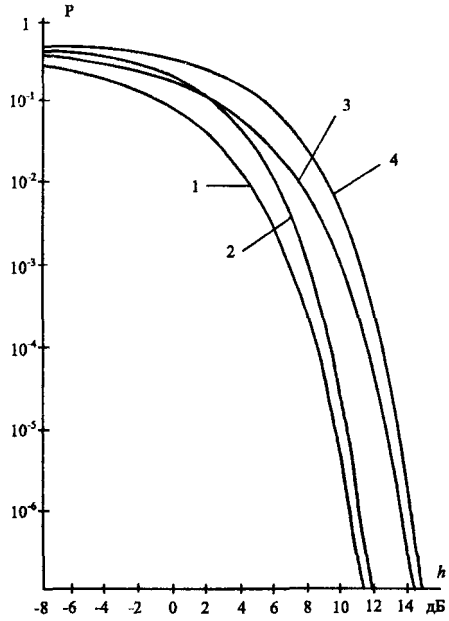

Fig. 1. Dependence of error probability P on the relation of signal power to noise power h

The error probability $P_{ош}$ in the relation of signal power to noise power h is presented by dependence (3) for incoherent reception of the FM signal:

$$P_{ош} = \frac{1}{2} e^{-h/2}. \tag{3}$$

Dependence of probability of a binary PM signal on the relation of energy of a signal to spectral density of noise power for coherent reception [2], [3]:

$$P_e = 1 - F\left[\sqrt{\frac{2E(s)}{N_0}}\right]. \tag{4}$$

Dependence of probability orthogonal FM signals on a time interval [0, T] under condition of equality of energy of signals [2]:

$$P_e = 1 - F\left[\sqrt{\frac{E_s}{N_0}}\right]. \tag{5}$$

Formation of orthogonal FM and opposite PM signals is based on specific laws.

It is follows from a number of works, that the binary system of signals with phase manipulation has the best noise immunity at coherent reception. The signal/noise relation of such system is

$$h_2 = \sqrt{2E/N_0}, \tag{6}$$

At $E_2 = E_0 = E_1$, where N_0 – spectral density of noise power.

Advantages of PM decrease when $M > 2$ because of the mutual influence caused by cross correlation between signals.

The initial phase is unknown and is a random variable at incoherent reception. The greatest noise immunity corresponds to transfer of the binary information by orthogonal signals. The error probability at not coherent reception of two orthogonal signals [1], [2]:

$$P_{ou} = 0{,}5\exp(-0{,}5h_2^2). \tag{7}$$

The noise immunity of coherent and incoherent reception of two orthogonal signals differs slightly.

From Shannon's equation for speed of transfer [3]

$$C = F\log_2\left(1+\frac{P_c}{P_ш}\right), \tag{8}$$

where F – bandwidth; P_c – signal power; $P_ш$ – noise power.

The formula for speed of transfer is represented under condition of uniform spectral density of noise and $P_c << P_ш$:

$$C = {}^{P_c}\!/_{N_0}\ln 2, \tag{9}$$

then $\ln 2 = {}^{P_c}\!/_{RN_0}$ duration of a m symbol of code sequence from k binary symbols [2]:

$$T_m = kT_2 = \frac{k}{R} = {}^{\log m}\!/_{R}. \tag{10}$$

FM symbols are transferred in multiposition system with various values of frequency. Incoherent reception of orthogonal signals FM in the area of normalized signal/noise relation on binary unit γ_2 (dB) is less than 0 dB. Incoherent reception has the same dependence on probability of erroneous reception P. In that case the binary system ($m = 2$) has advantage in comparison with systems when $m > 2$.

The probability of erroneous reception tends to zero exponentially. It is true when the signal/noise relation on binary unit satisfies the inequality [1]:

$$\gamma_2 > 2\ln 2. \tag{11}$$

Systems of signals possess threshold effect. At threshold values if energy of a signal on a binary symbol 1,39 times exceeds the power of spectral density of noise it is possible to use a binary orthogonal signal as a measure in the information leakage channel. A binary orthogonal signal has its advantages. It is sensitive and nonsynchronous.

It is offered to use binary orthogonal coherent and not coherent signals as a measure for an estimation of security of digital channels of information leakage. Dependence of probability of an error on the relation of capacity of a signal to capacity of noise of such signals is close to Shannon's border.

REFERENCES

1. 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.

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

3. 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.

4. Железняк, В.К. Основы теории модулированных колебаний: учебное пособие / В.К. Железняк, С.В. Дворников. – СПб.: ГУАП, 2006. – 160 с.